Attorney Docket No.: M-9793 US
First Inventor: Timothy R. Feldman
Title: A Secure Access Method and System

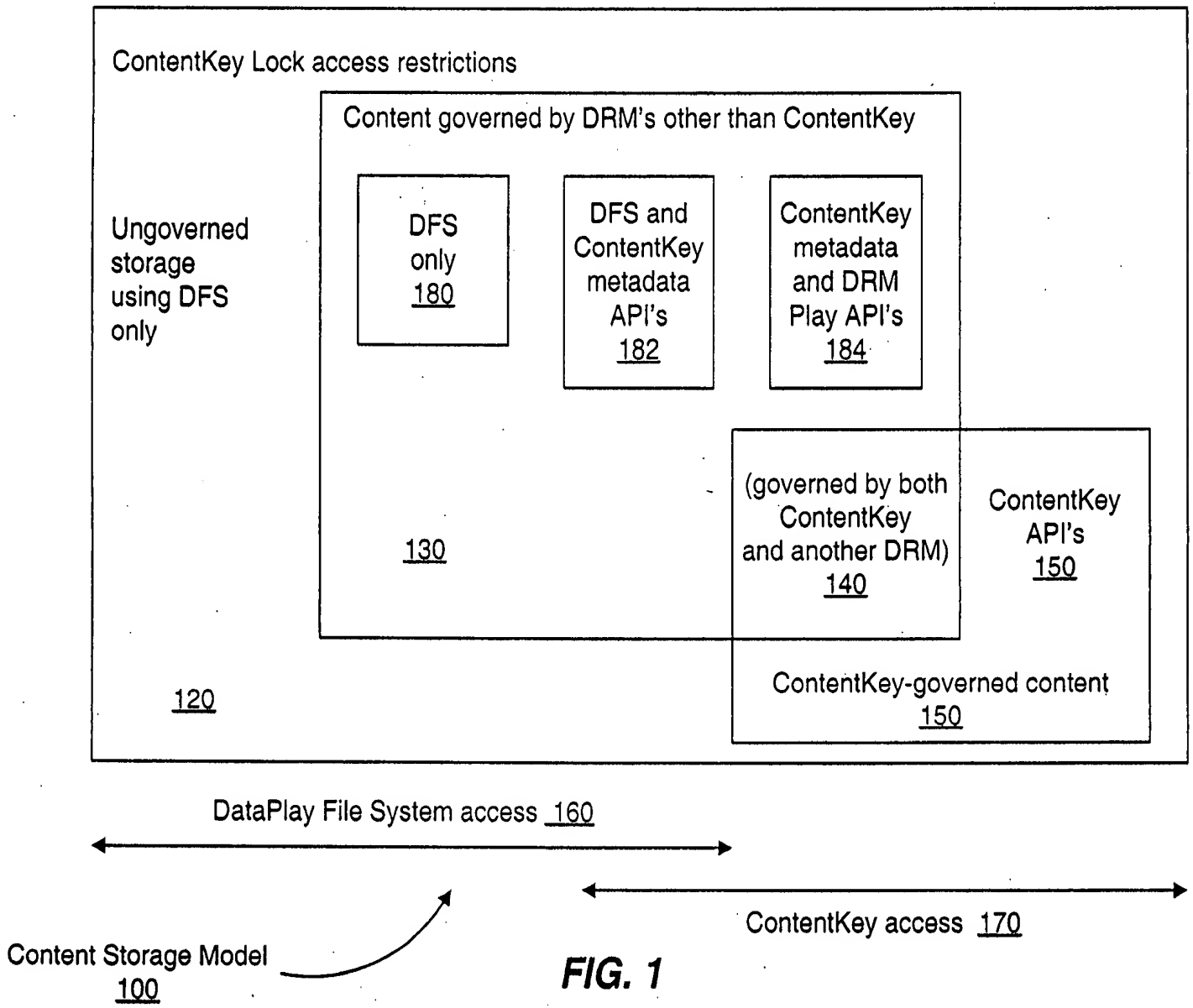

FIG. 1

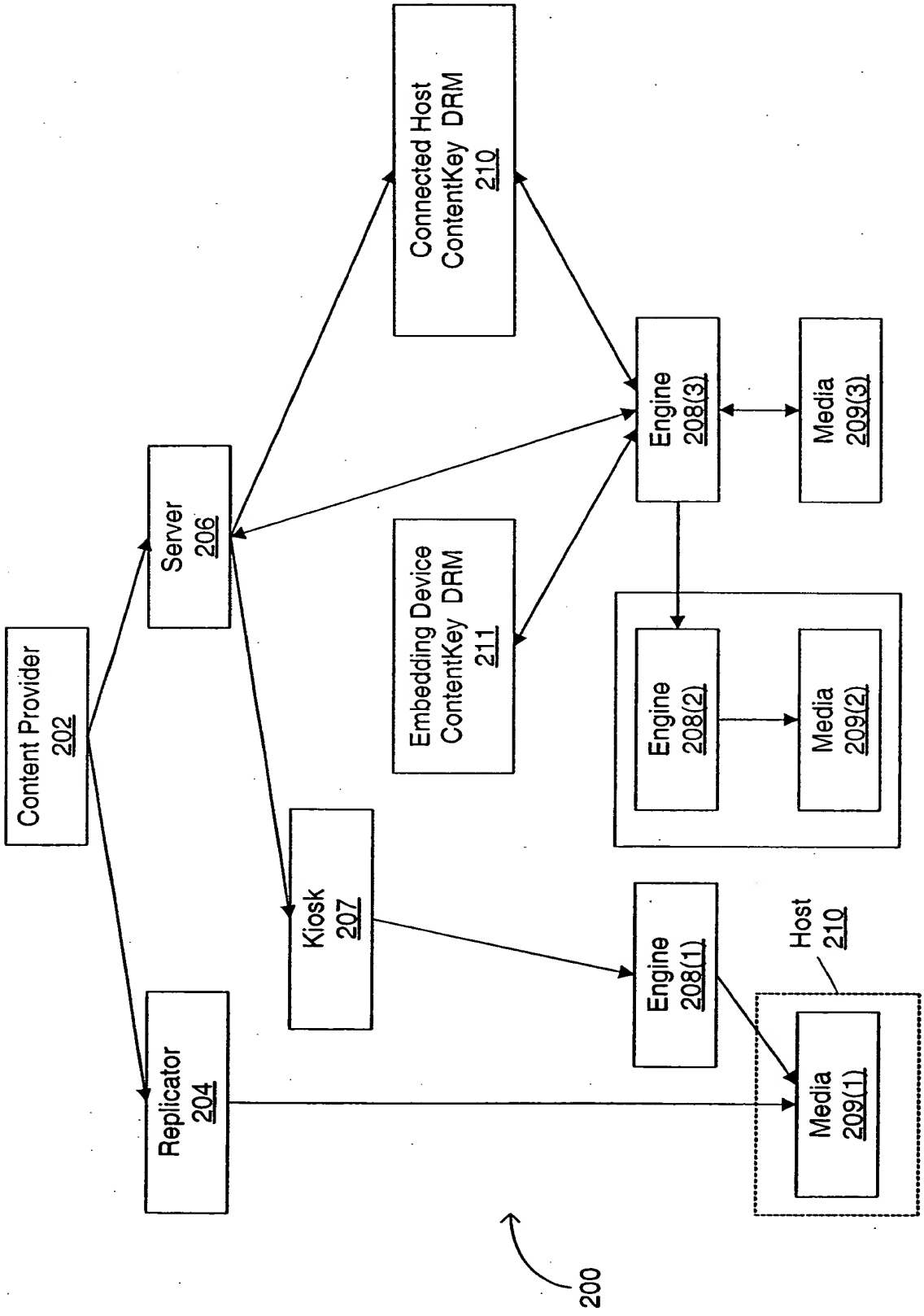
Content Provider 202
Server 206
Connected Host ContentKey DRM 210
Embedding Device ContentKey DRM 211
Engine 208(3)
Media 209(3)
Engine 208(2)
Media 209(2)
Kiosk 207
Engine 208(1)
Host 210
Media 209(1)
Replicator 204
200

FIG. 2

10/29/2004 08:00:00

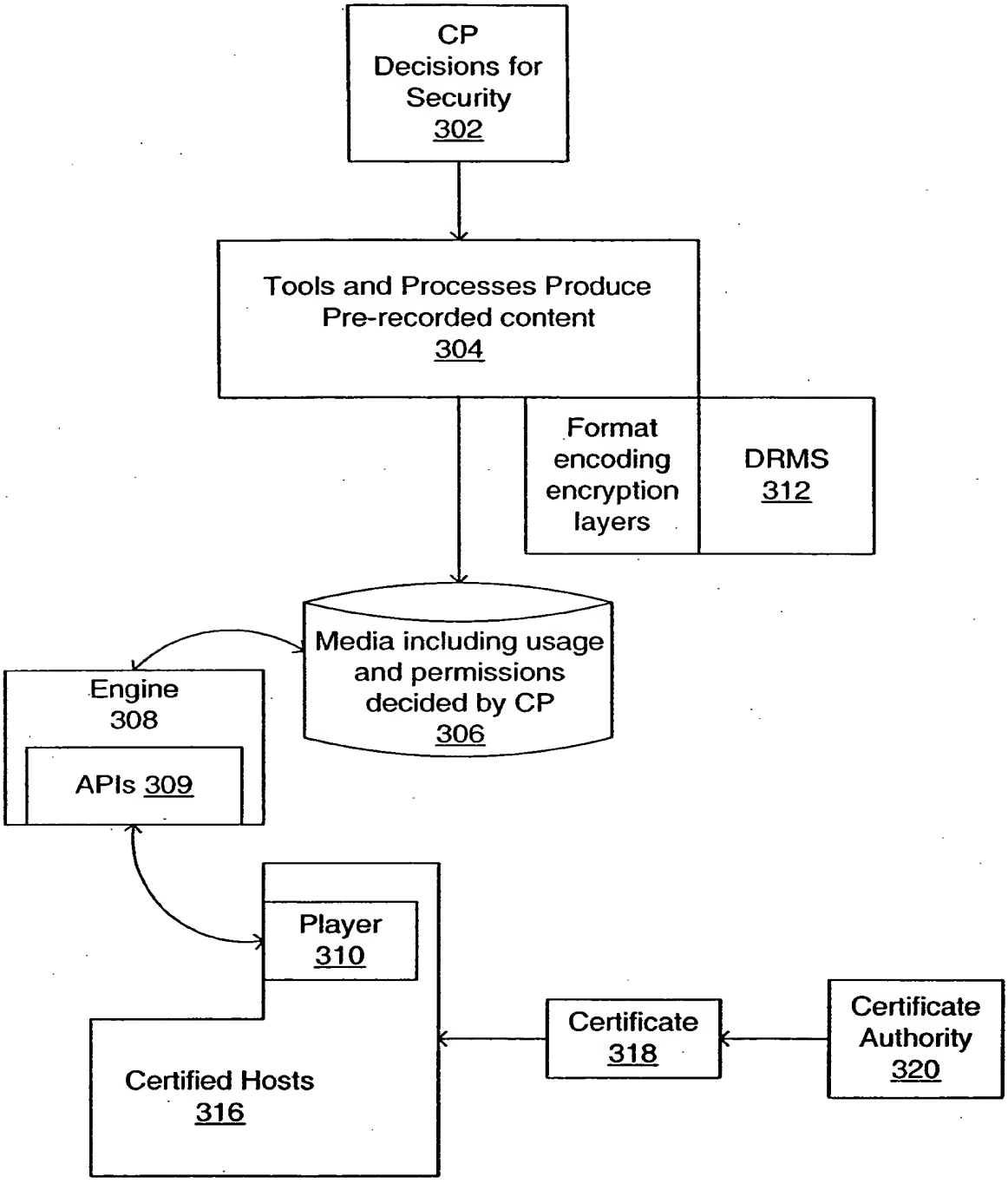

FIG. 3

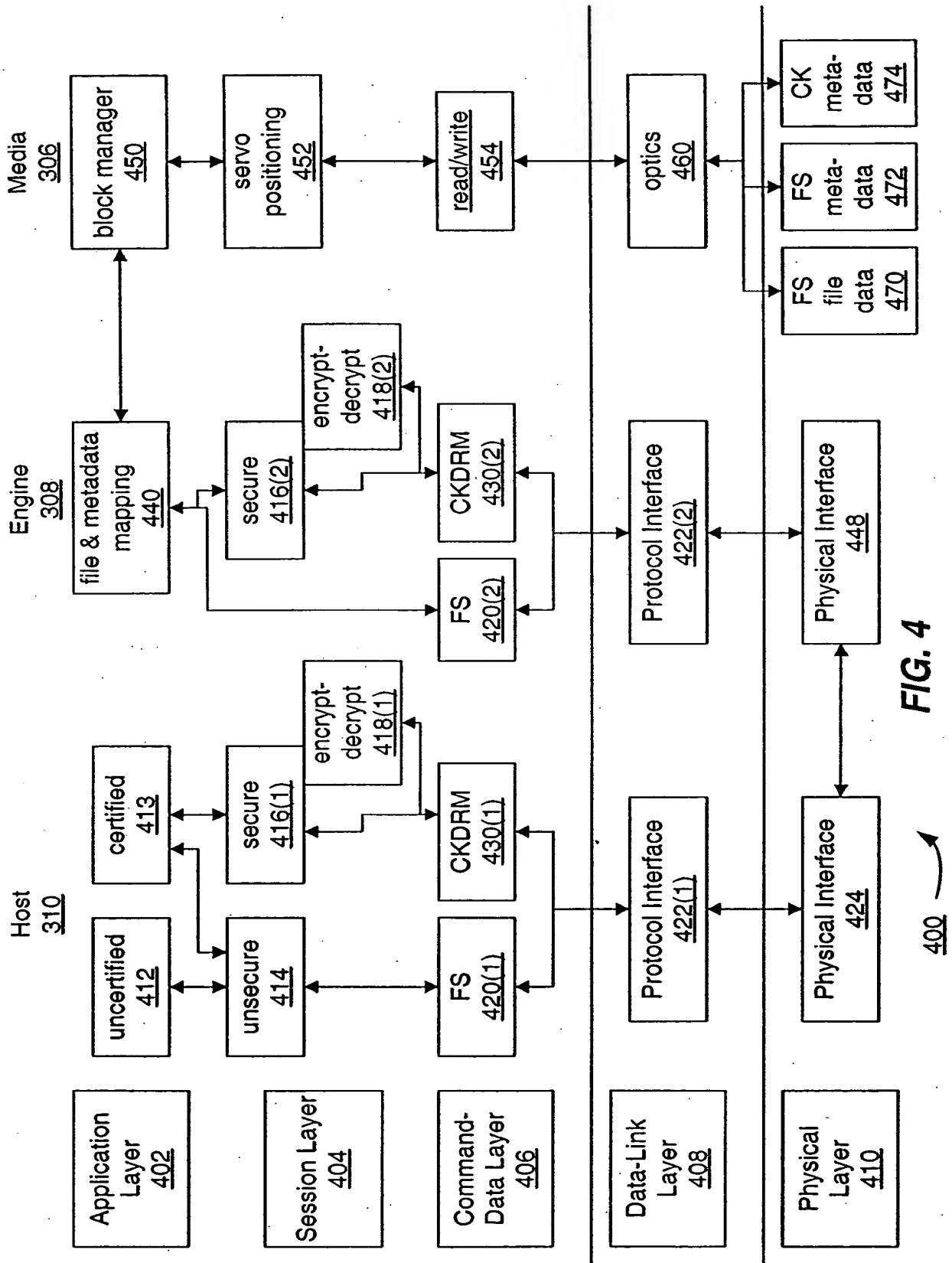
Application Layer 402
Session Layer 404
Command-Data Layer 406
Data-Link Layer 408
Physical Layer 410
Host 310
uncertified 412
certified 413
unsecure 414
secure 416(1)
encrypt-decrypt 418(1)
FS 420(1)
CKDRM 430(1)
Protocol Interface 422(1)
Physical Interface 424
Engine 308
file & metadata mapping 440
secure 416(2)
encrypt-decrypt 418(2)
FS 420(2)
CKDRM 430(2)
Protocol Interface 422(2)
Physical Interface 448
Media 306
block manager 450
servo positioning 452
read/write 454
optics 460
FS file data 470
FS meta-data 472
CK meta-data 474
400

FIG. 4

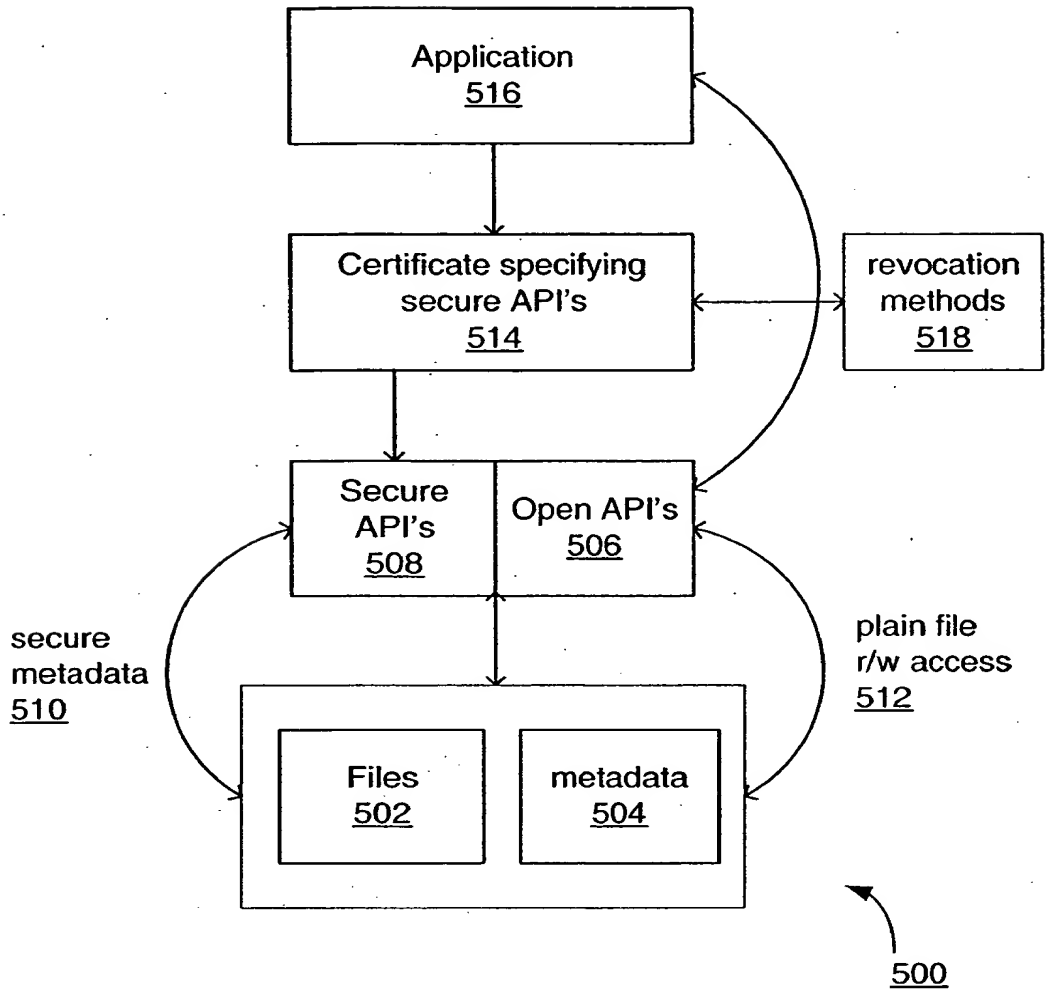

FIG. 5A

Petitioner's Exhibit 1002
Page 0096

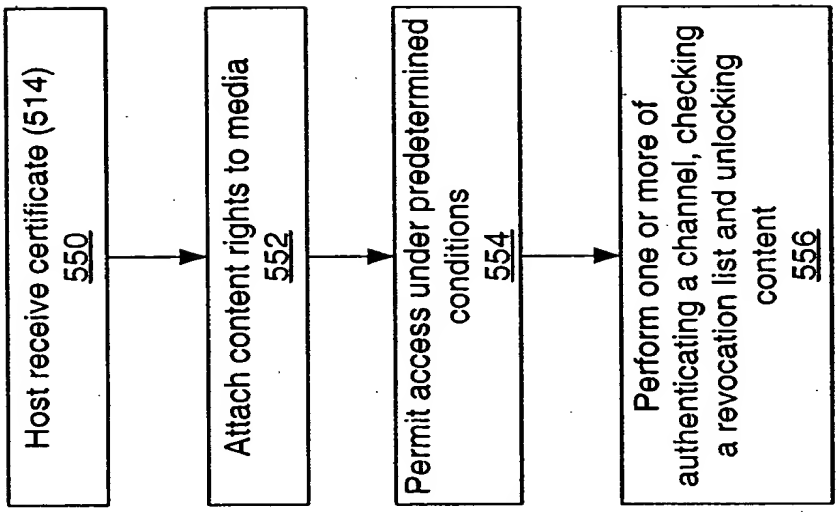

FIG. 5C

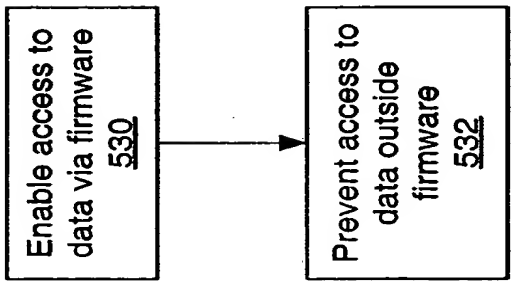

FIG. 5B

TO/2360 "E804h560

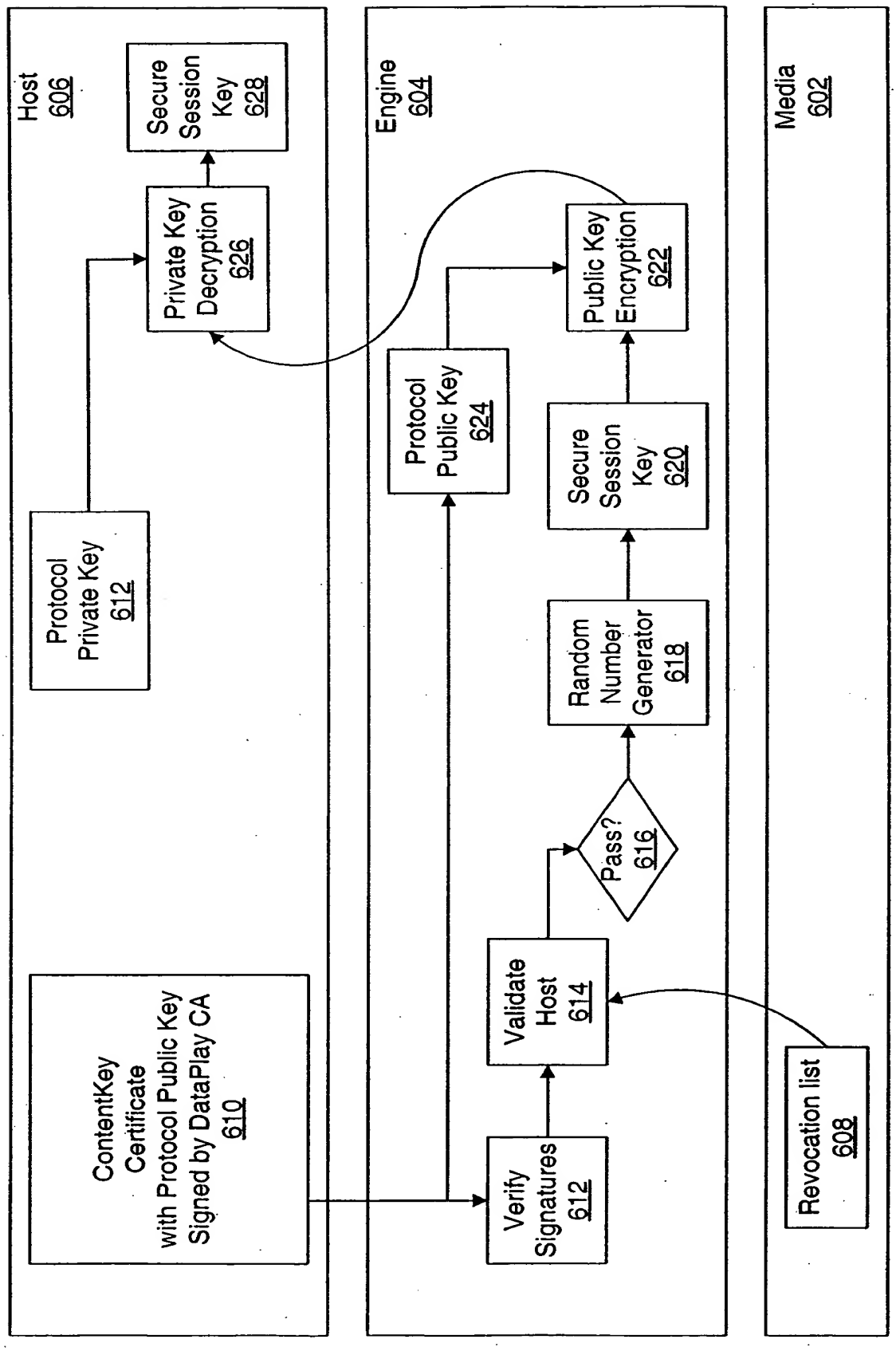
Host 606
Secure Session Key 628
Private Key Decryption 626
Protocol Private Key 612
ContentKey Certificate with Protocol Public Key Signed by DataPlay CA 610
Engine 604
Protocol Public Key 624
Public Key Encryption 622
Secure Session Key 620
Random Number Generator 618
Pass? 616
Validate Host 614
Verify Signatures 612
Media 602
Revocation list 608

FIG. 6

EV 338 948 760 US

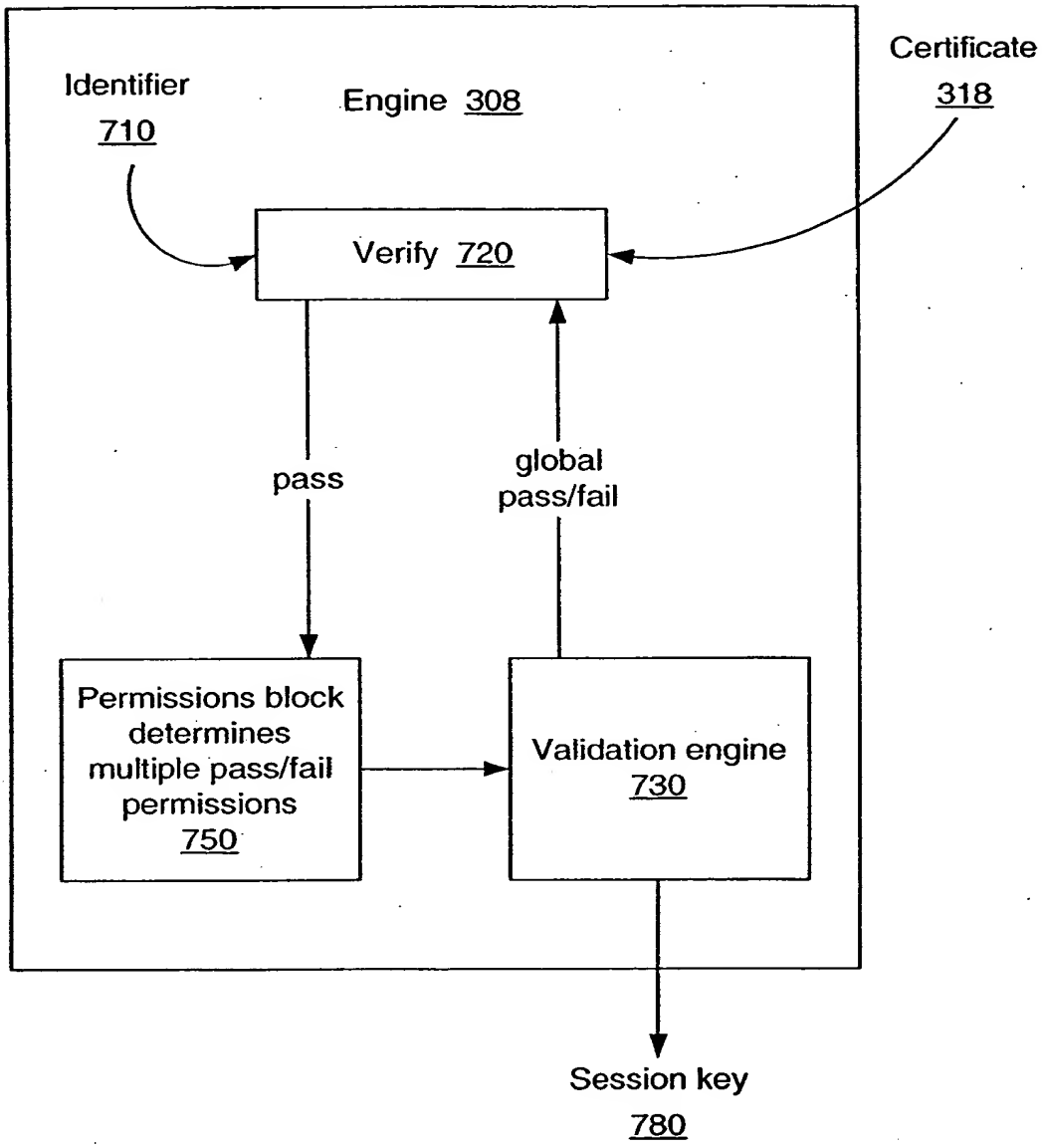

FIG. 7A

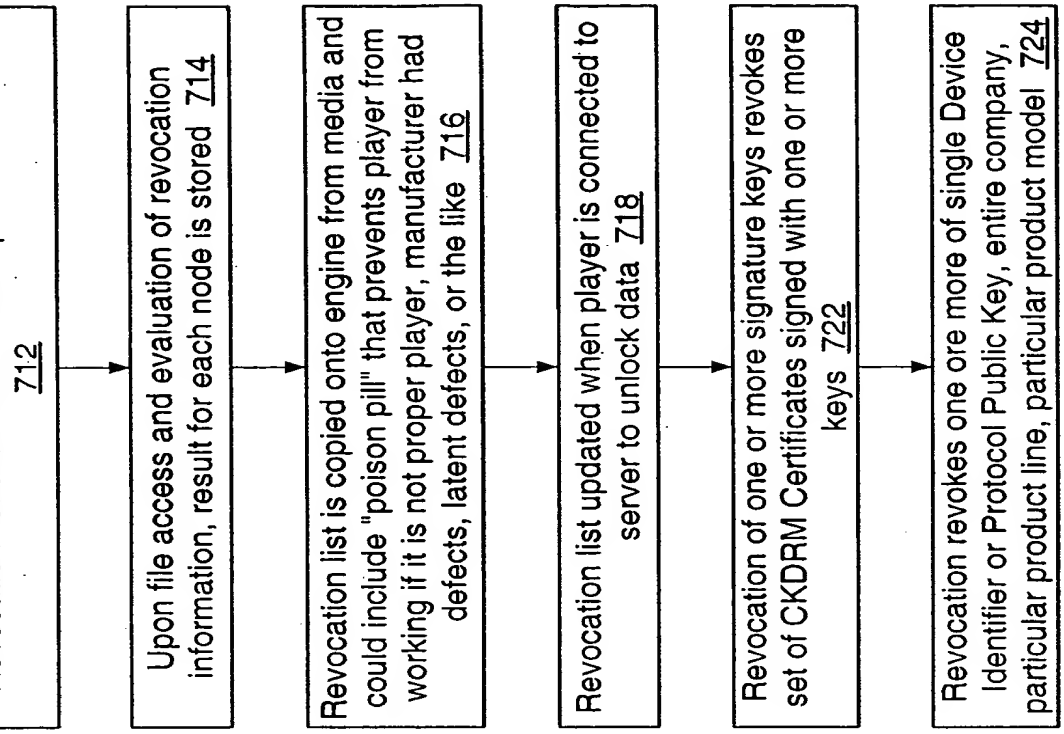
Revocation list evaluation made upon file access 712
Upon file access and evaluation of revocation information, result for each node is stored 714
Revocation list is copied onto engine from media and could include "poison pill" that prevents player from working if it is not proper player, manufacturer had defects, latent defects, or the like 716
Revocation list updated when player is connected to server to unlock data 718
Revocation of one or more signature keys revokes set of CKDRM Certificates signed with one or more keys 722
Revocation revokes one ore more of single Device Identifier or Protocol Public Key, entire company, particular product line, particular product model 724

FIG. 7C

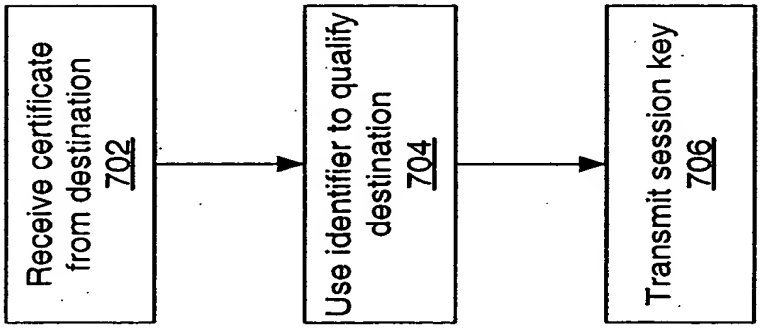
Receive certificate from destination 702
Use identifier to qualify destination 704
Transmit session key 706

FIG. 7B

T07280 E800h660

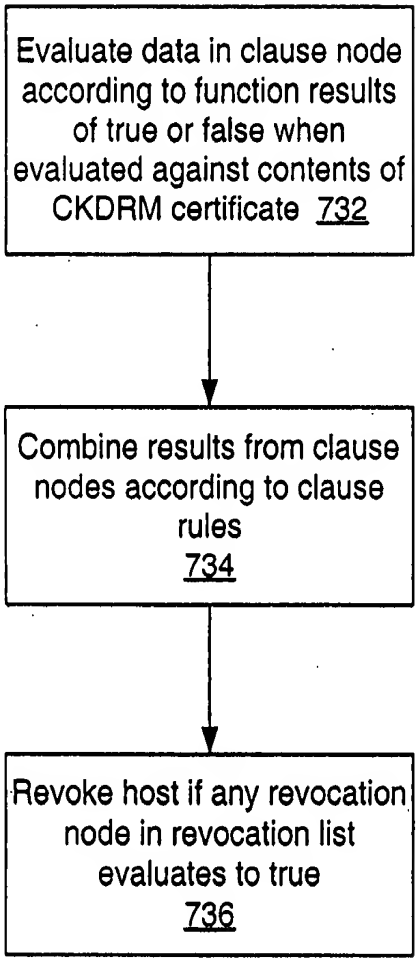

FIG. 7D

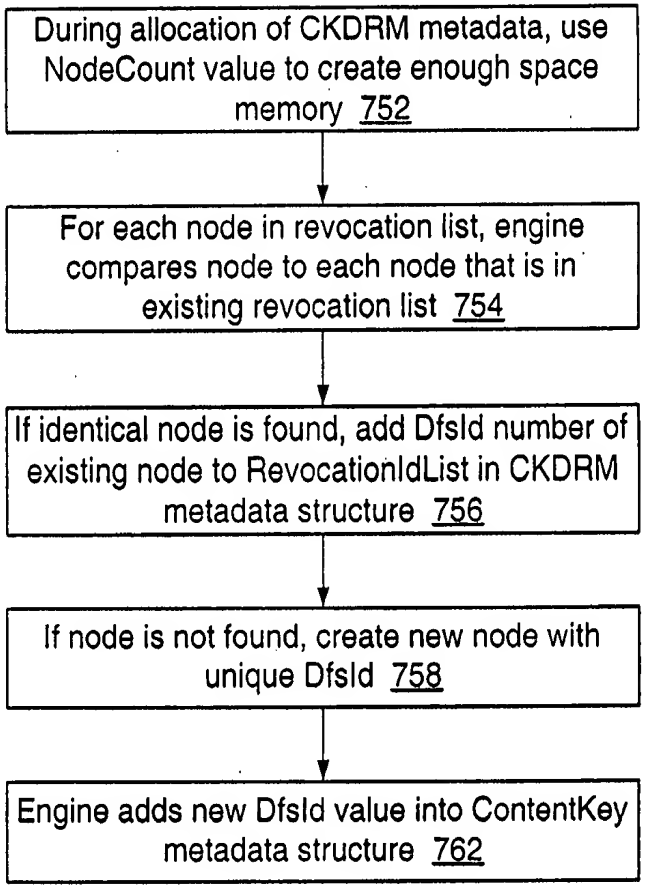

FIG. 7E

FD-2680-3808-4-50

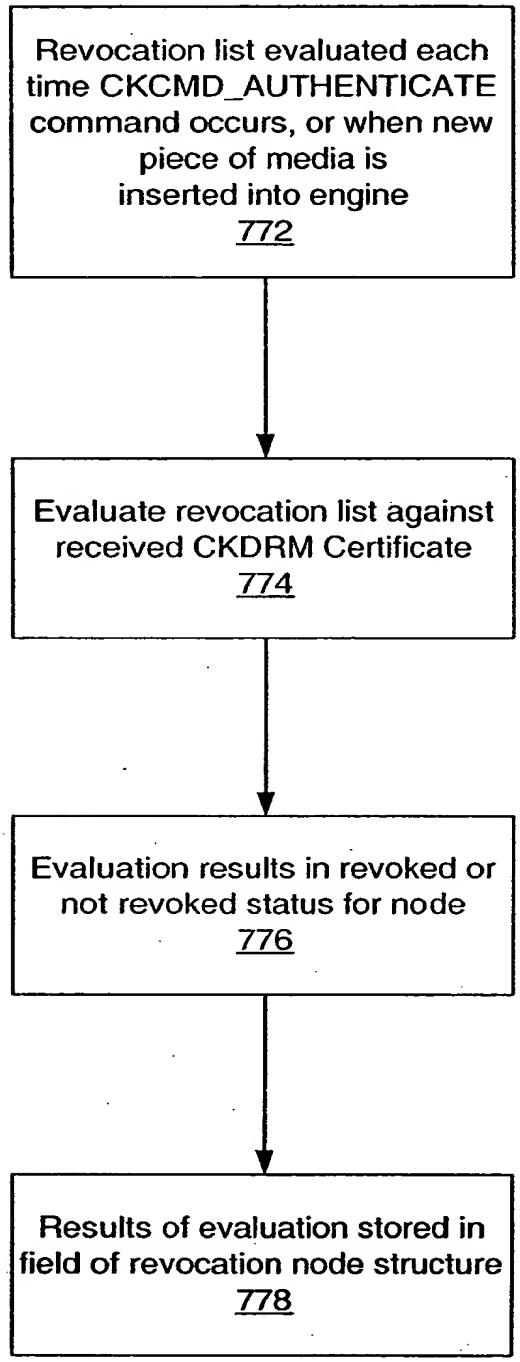

FIG. 7F

EV 730 380 460 US

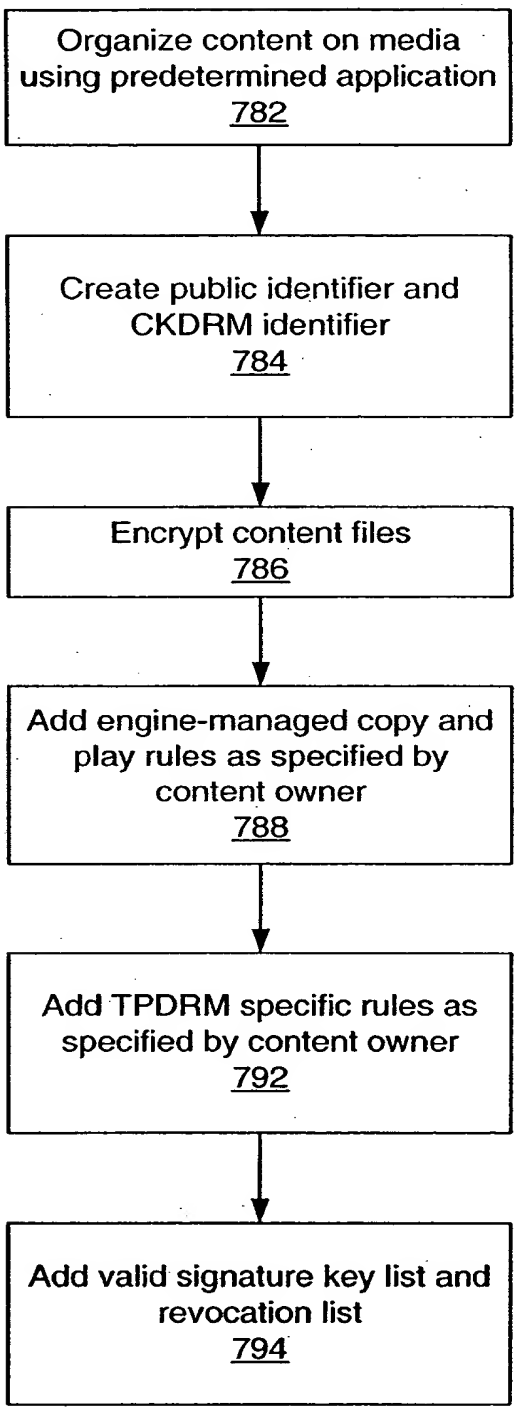

FIG. 7G

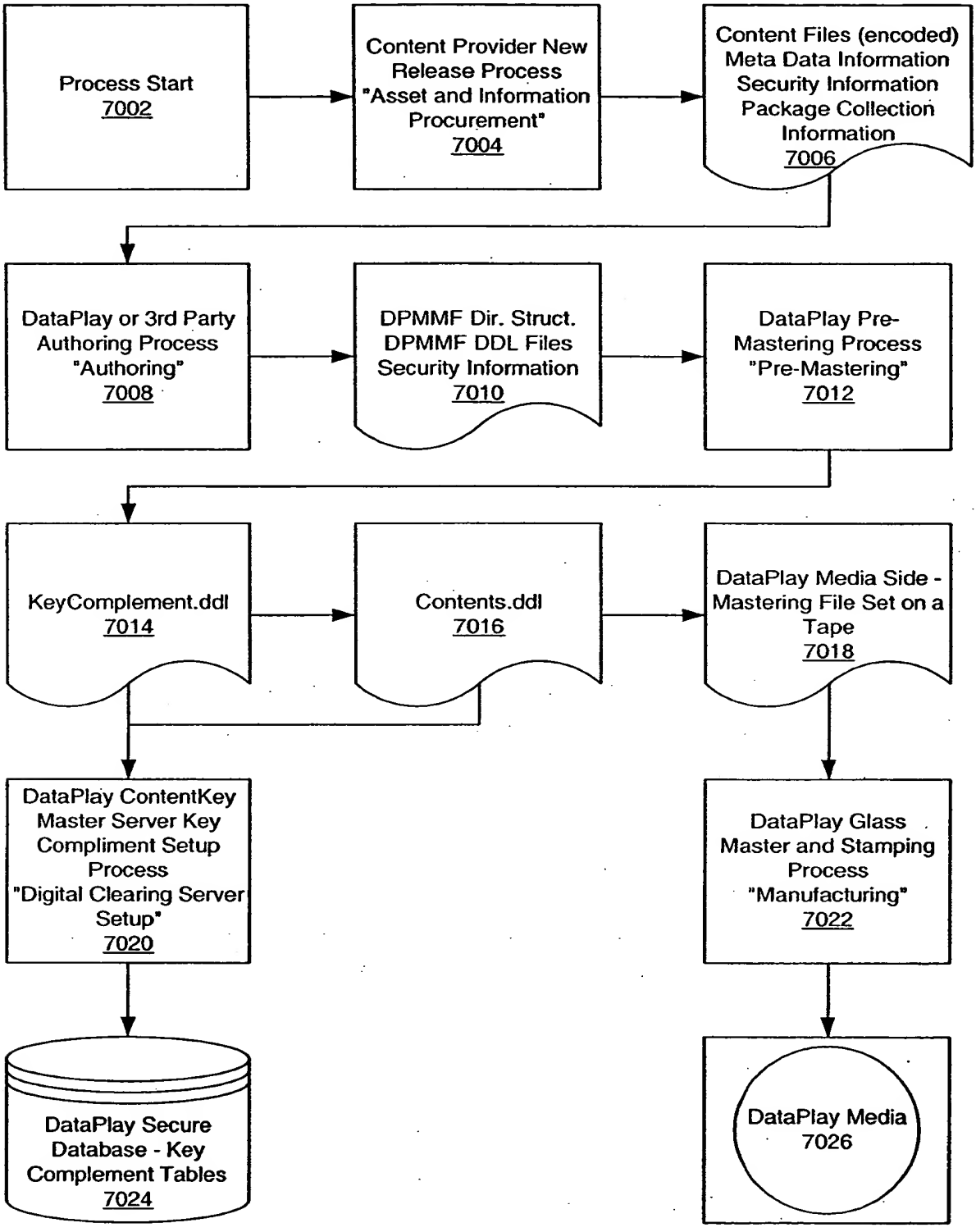

FIG. 7H

EL 278 380 465 US

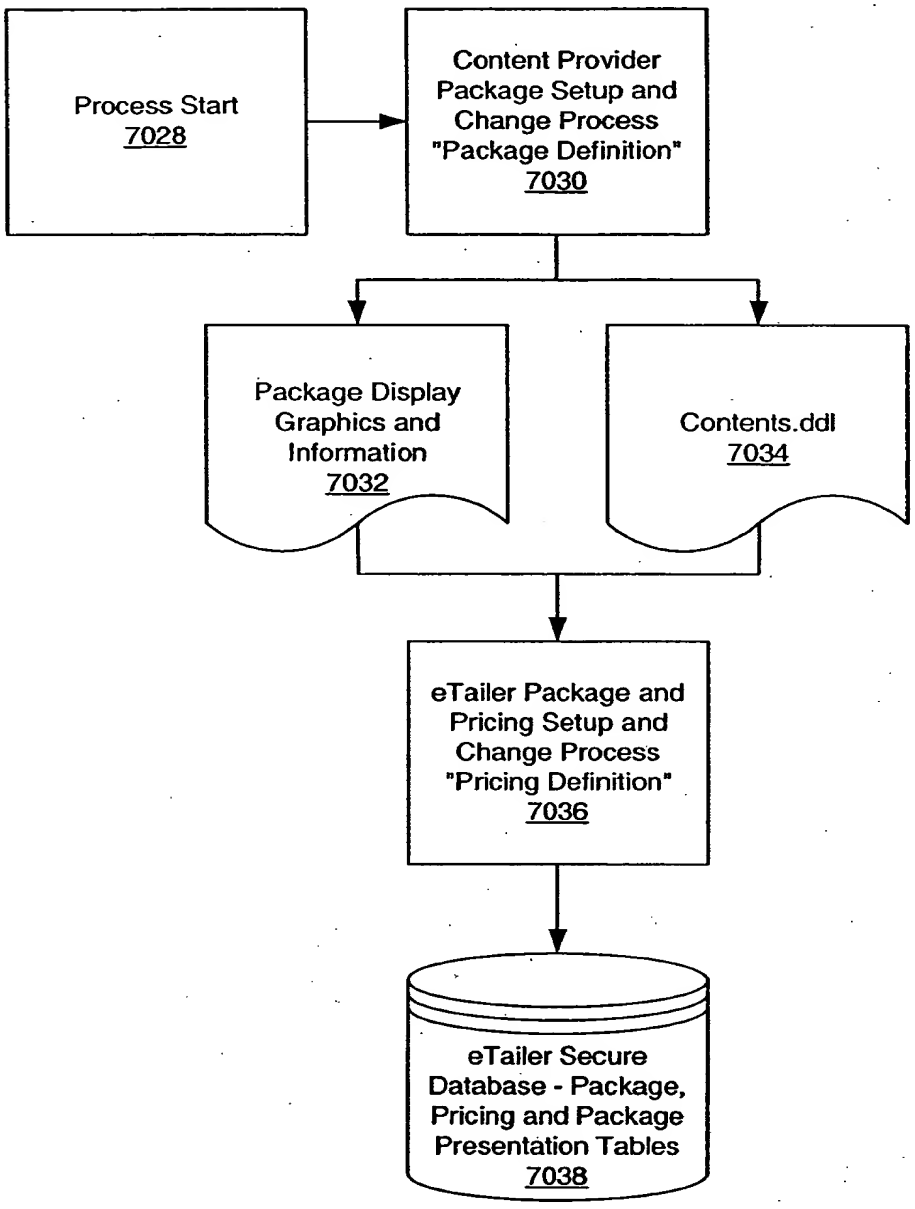

FIG. 7I

EV238038460

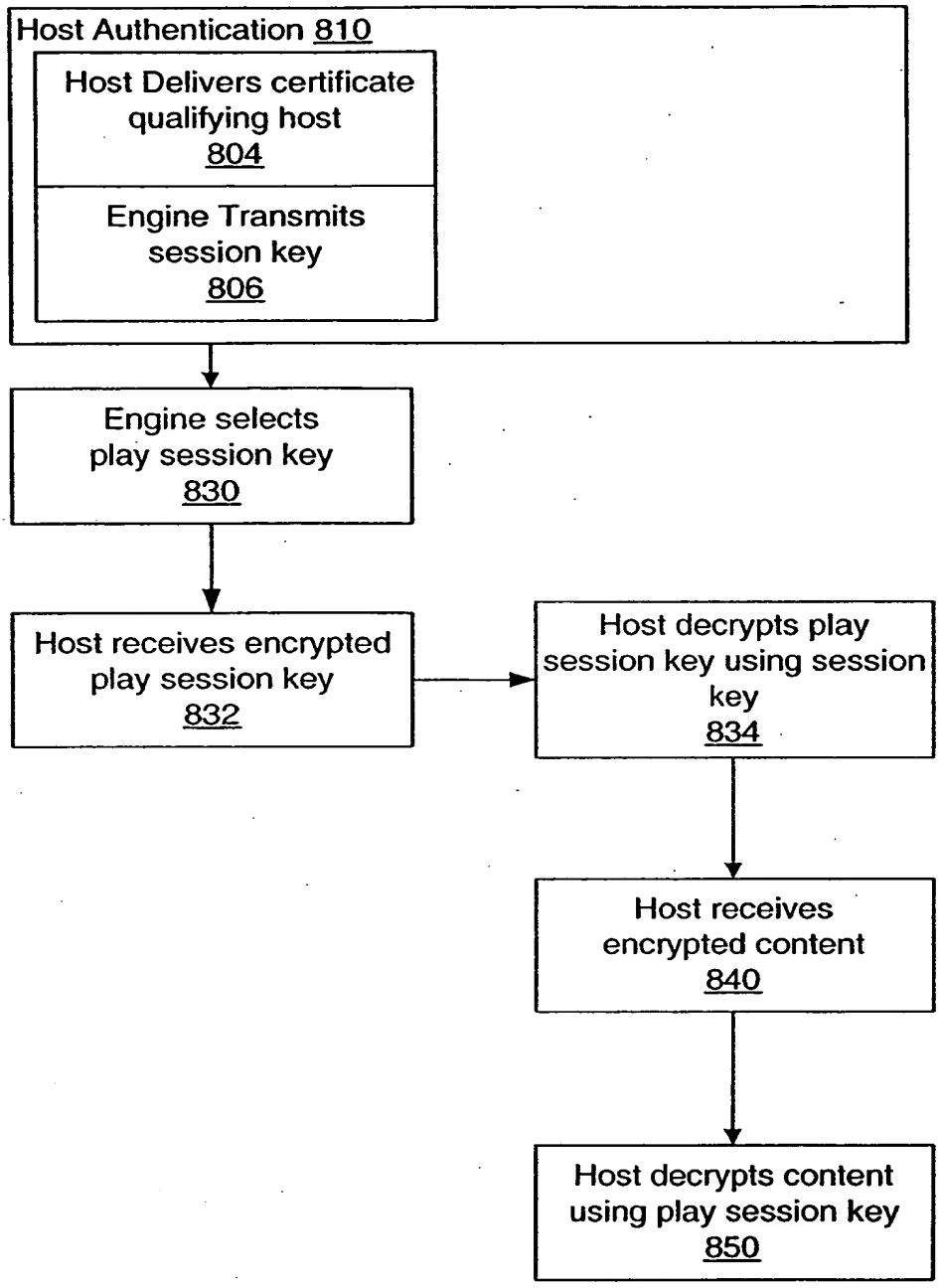

FIG. 8

EXPRESS MAIL NO. EV 329 368 704 US

EP 1 280 345 A2

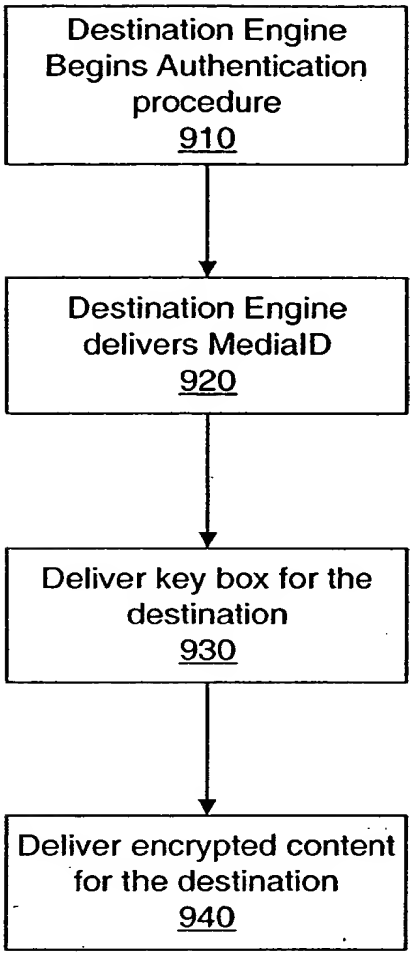

FIG. 9

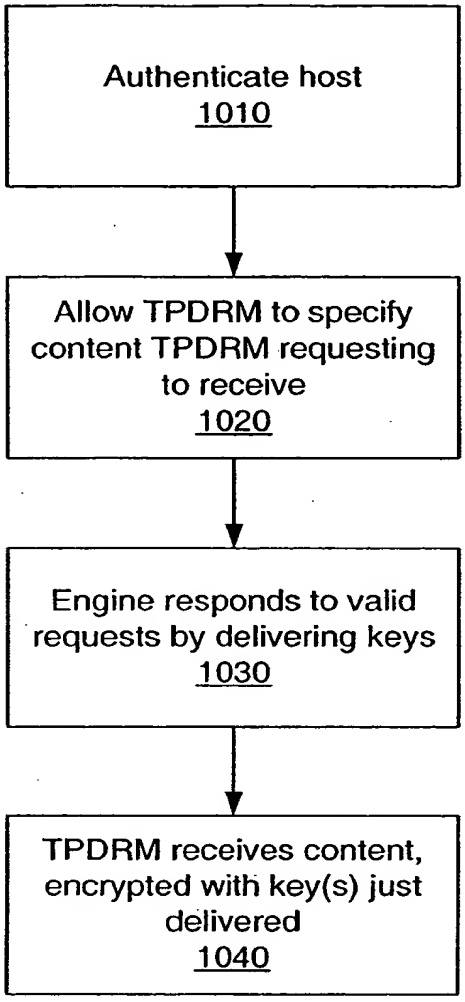

FIG. 10

Total pages: 8 of 46

TO2380 2800+60

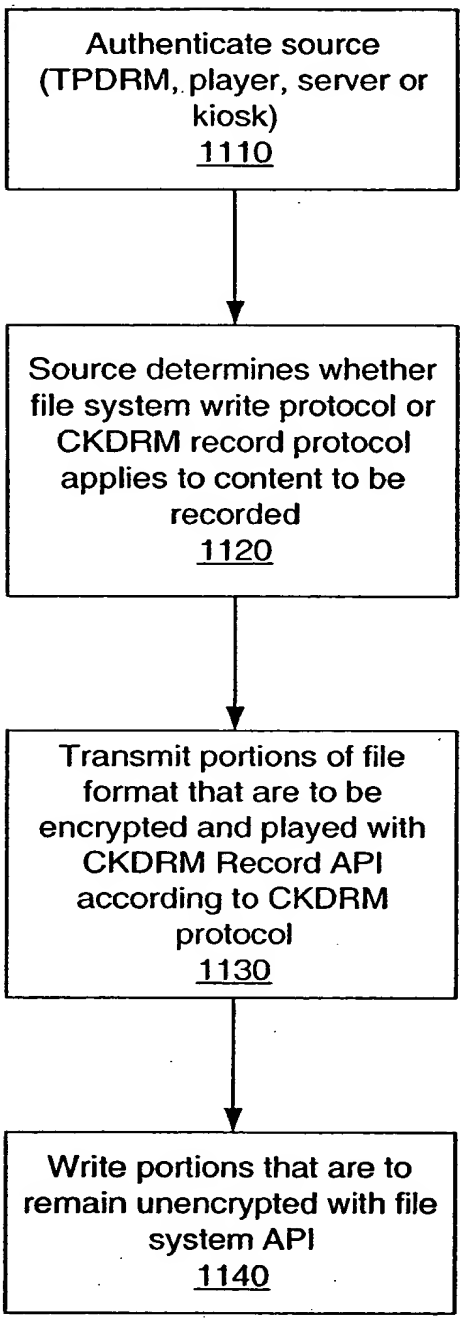

FIG. 11

TO/2880:S800+960

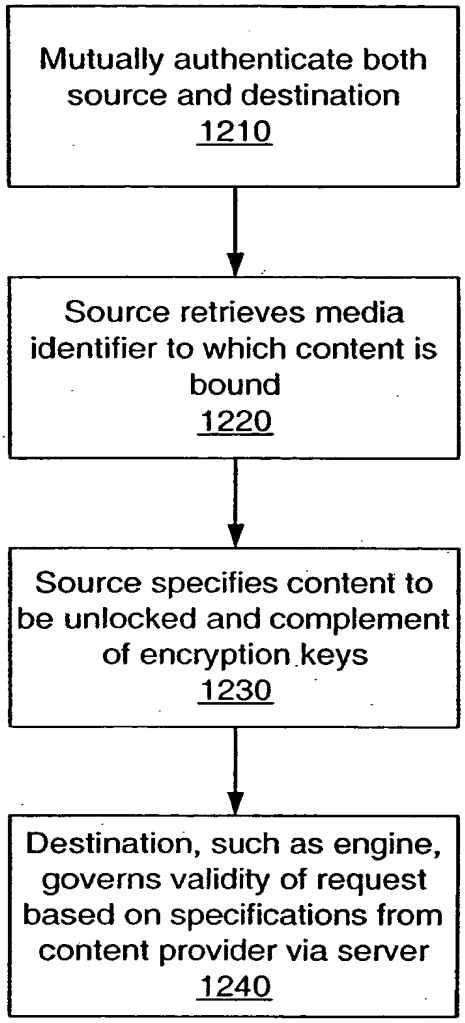

FIG. 12

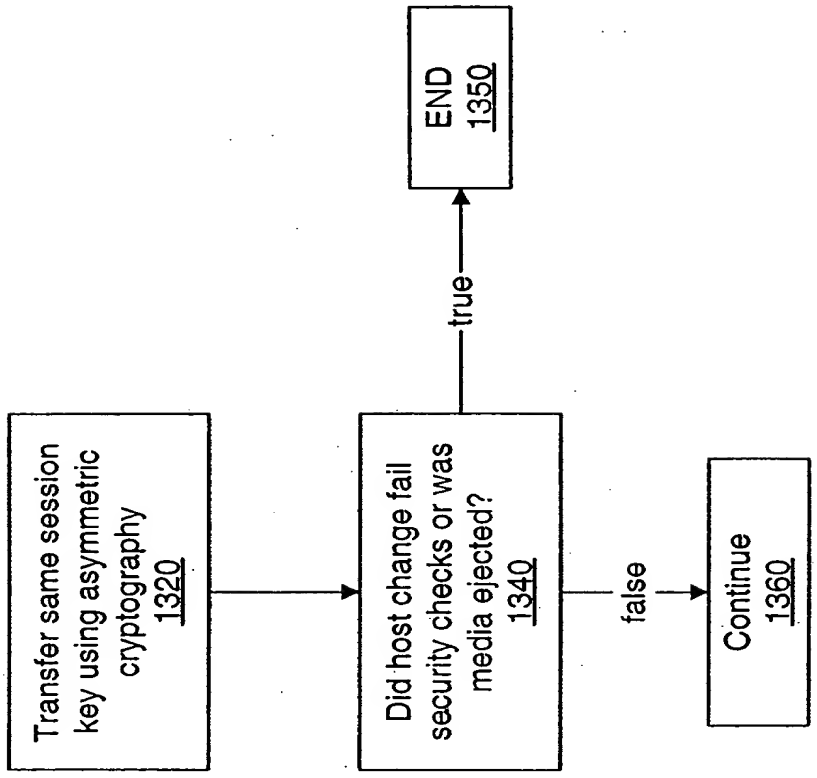
Transfer same session key using asymmetric cryptography 1320
Did host change fail security checks or was media ejected? 1340
true
END 1350
false
Continue 1360

FIG. 13

EQ/2180"E80046D

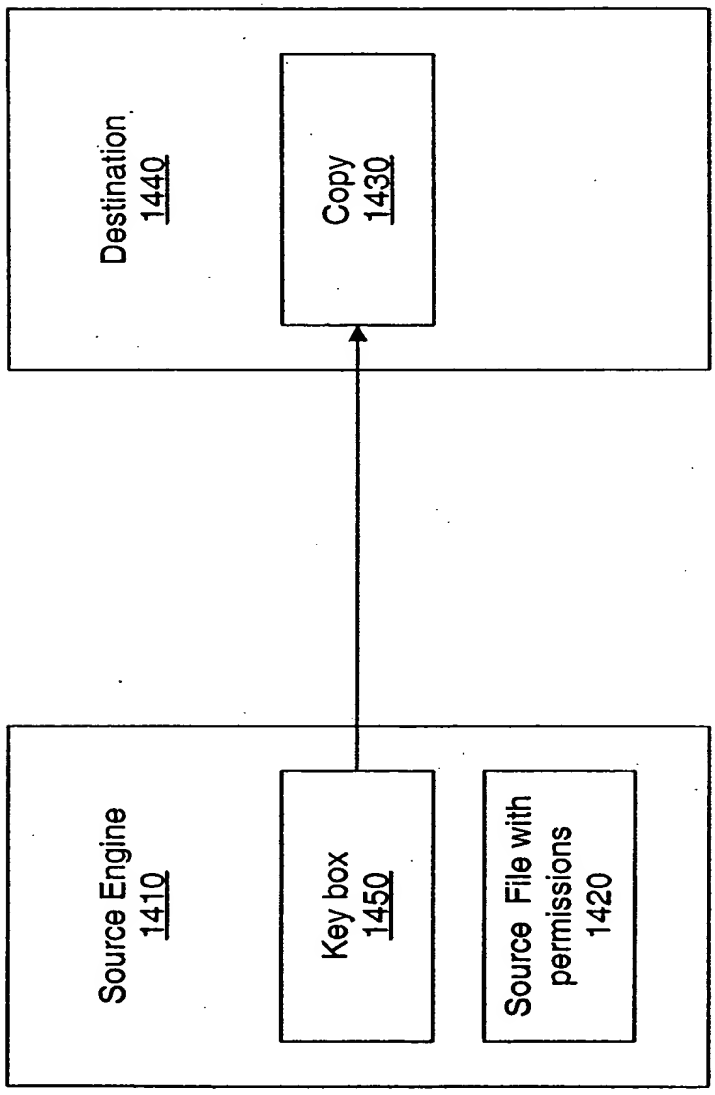

FIG. 14

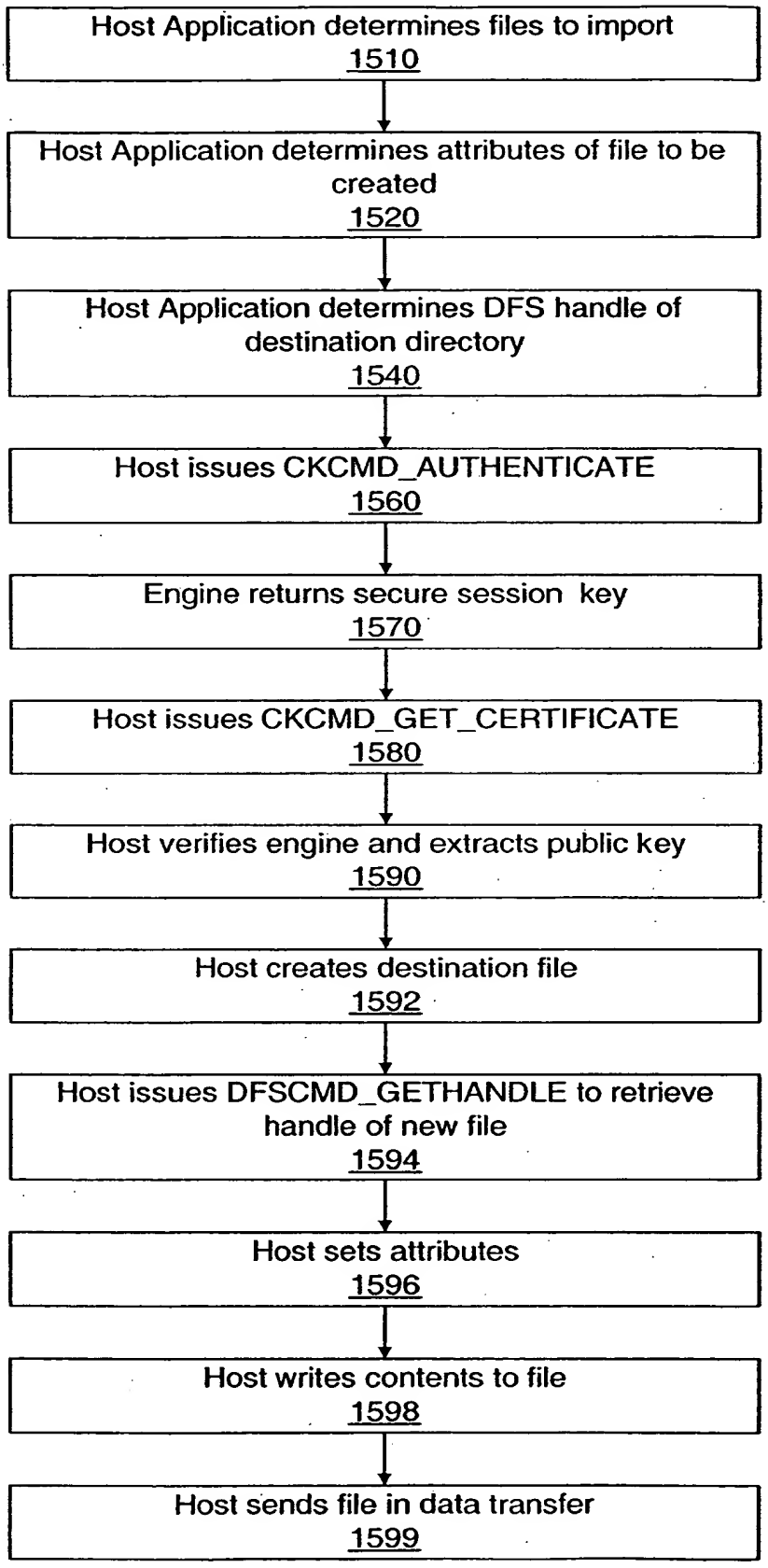

FIG. 15

EDV2380 v1.0 2003-08-15

EXPRESS MAIL NO. EV 339048659 US

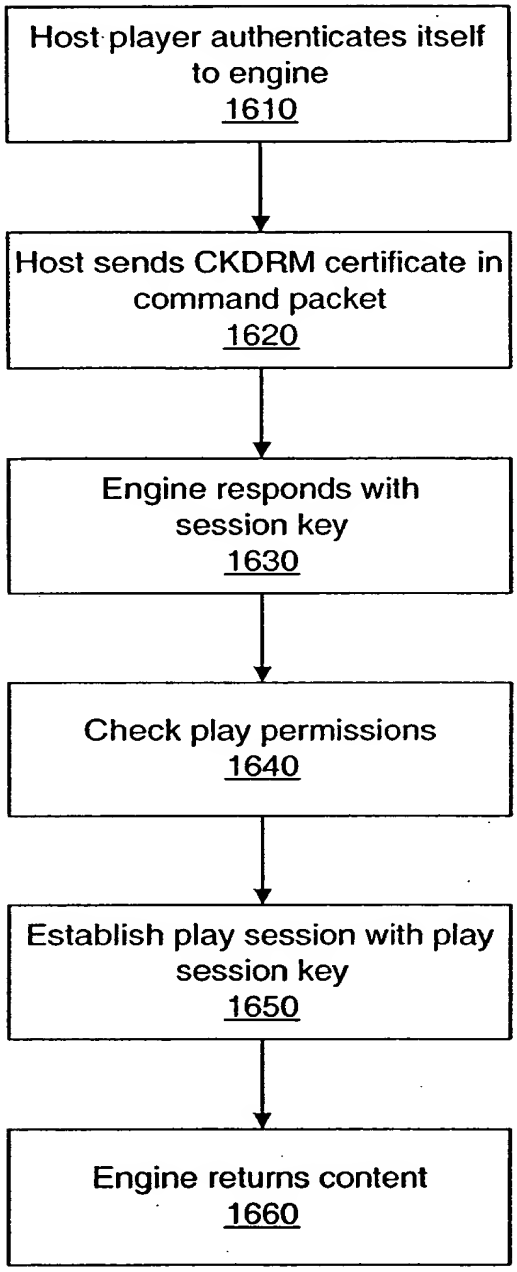

FIG. 16

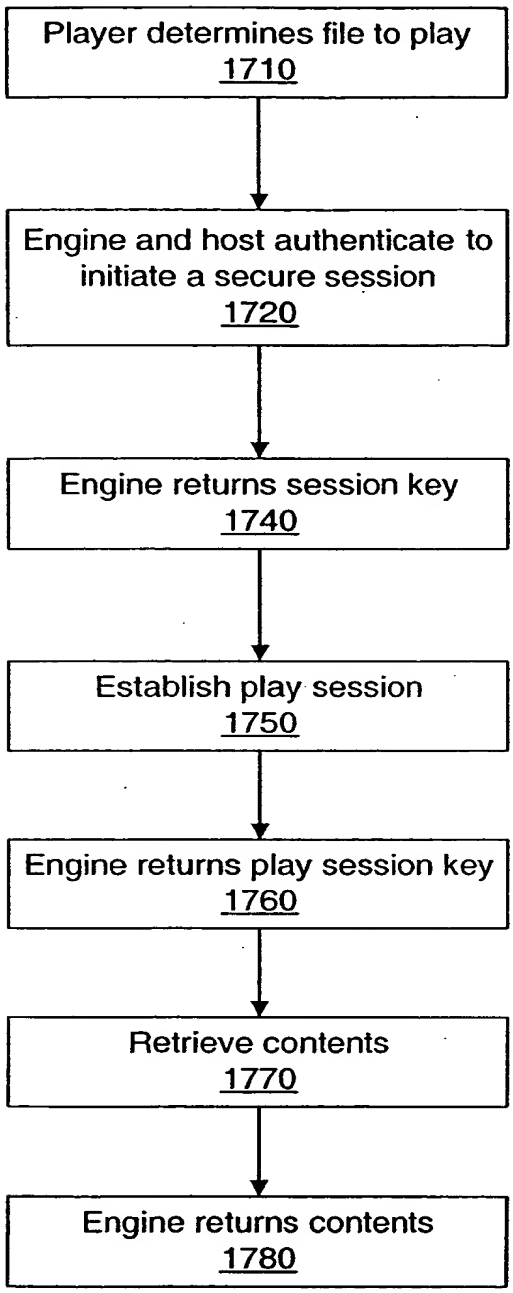

FIG. 17

Doc#: 08820704.1

10760701.060403

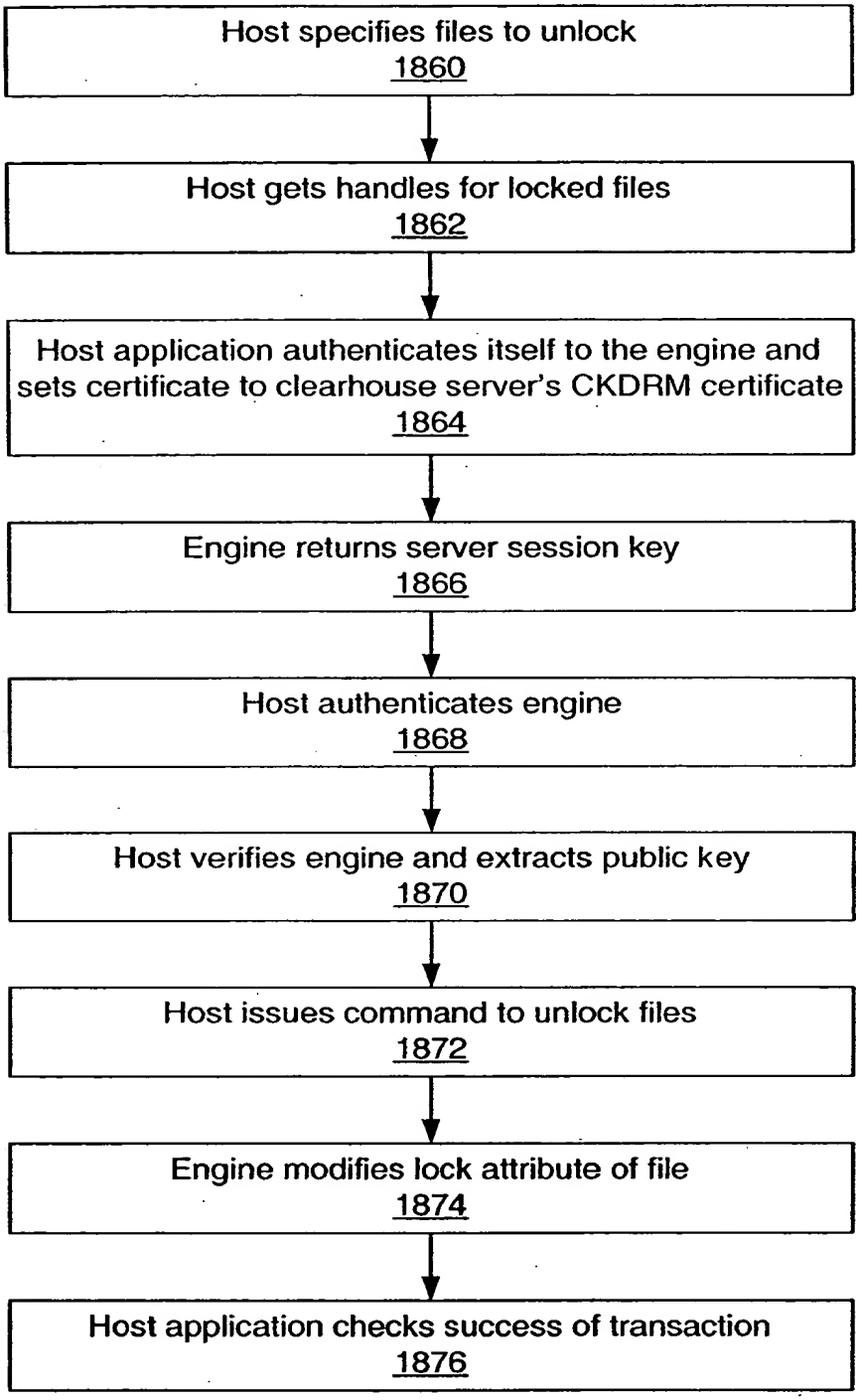

FIG. 18

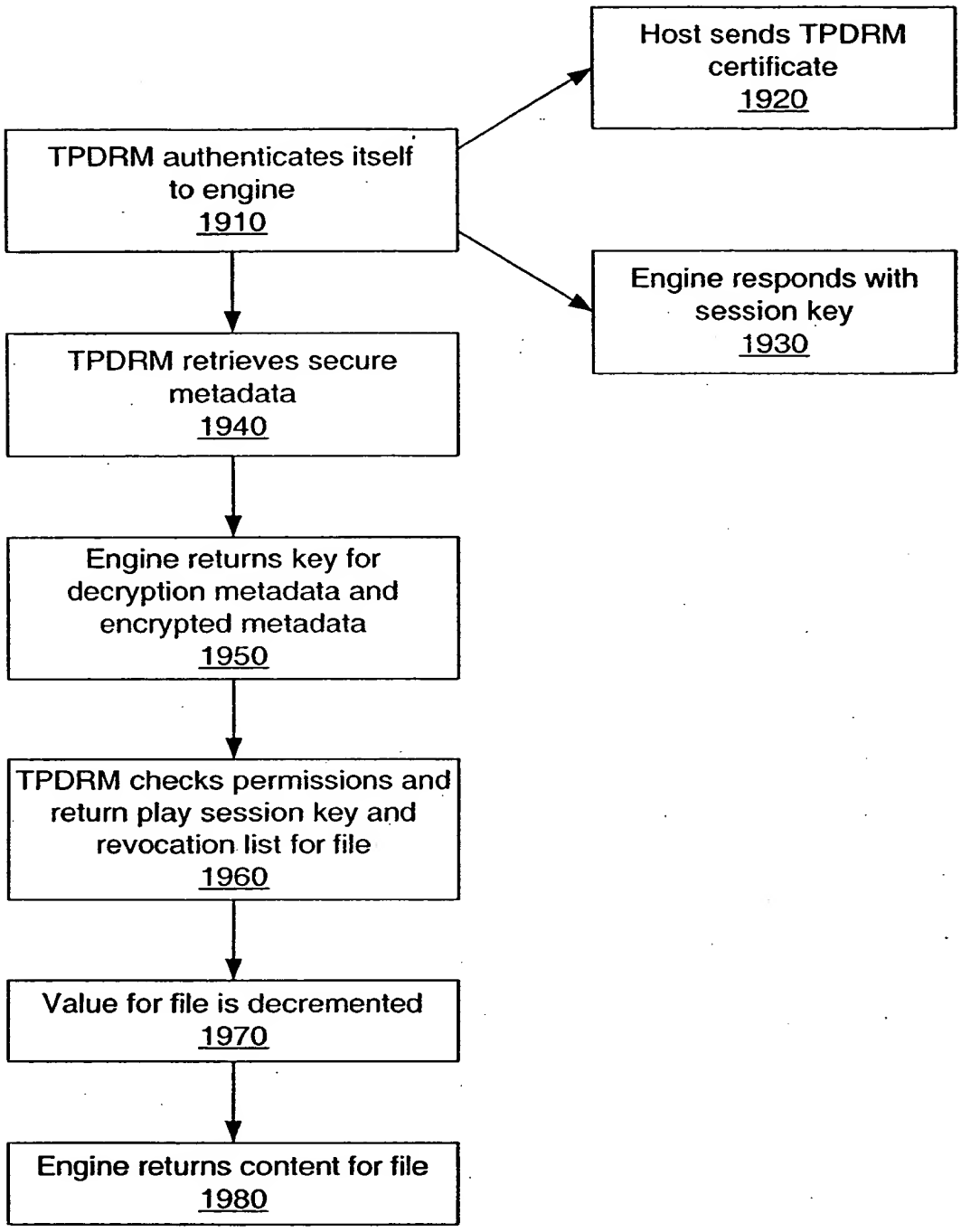

FIG. 19

EXPRESS MAIL NO. EV 280 398 040 US

EV 720 380 360 US

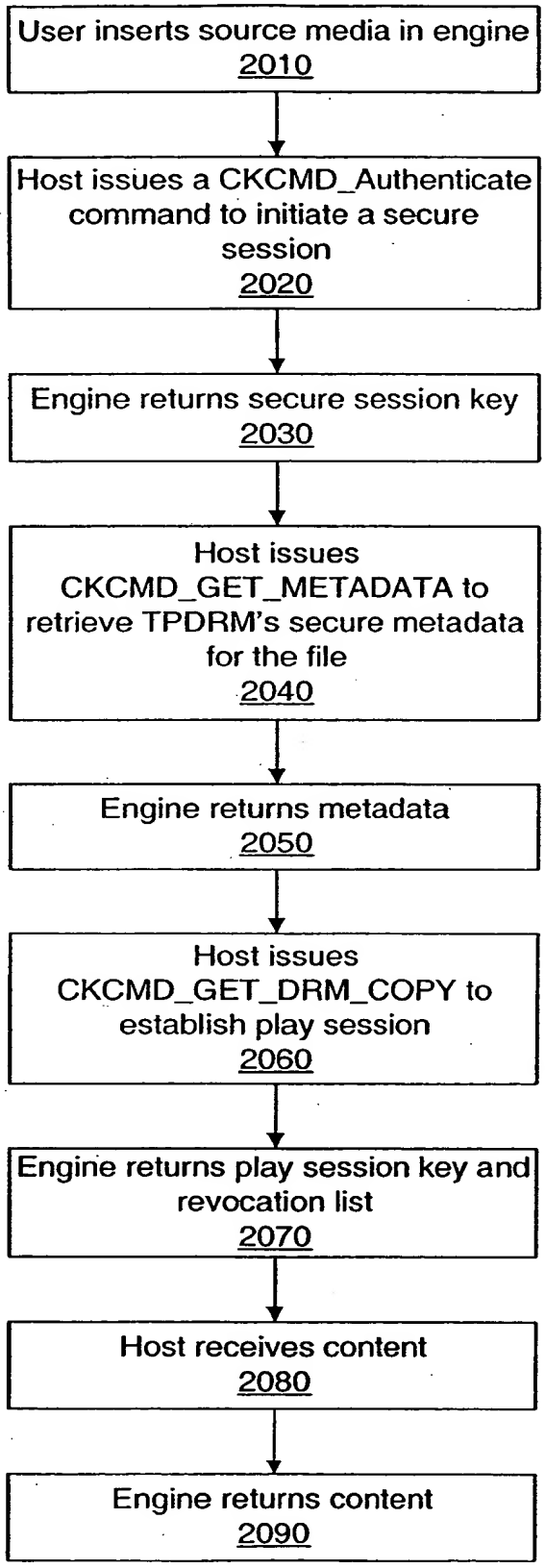

FIG. 20

EL279038004US60

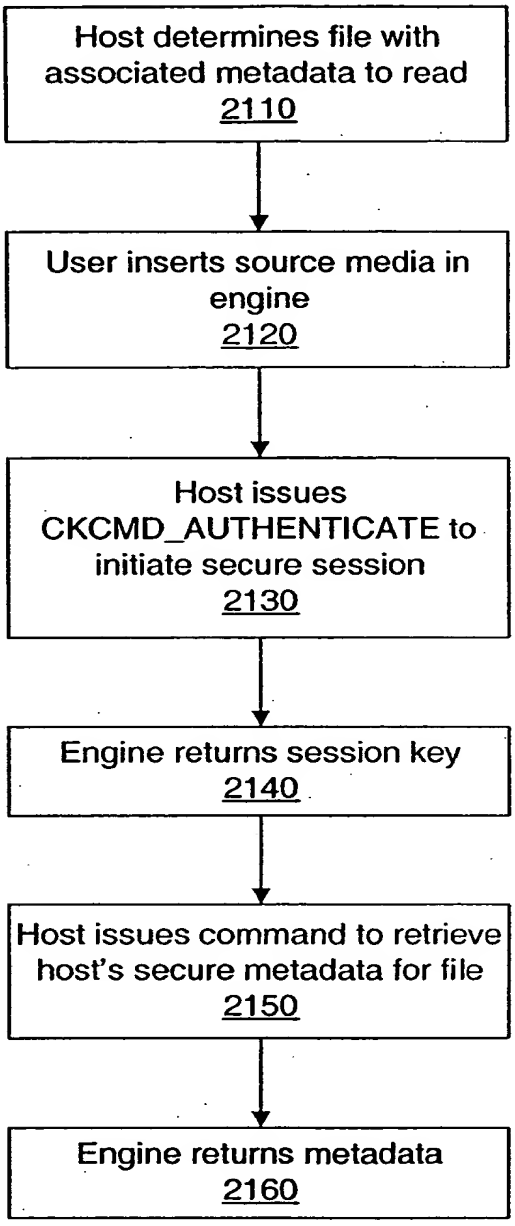

FIG. 21

EXPRESS MAIL NO. EV 339048760 US

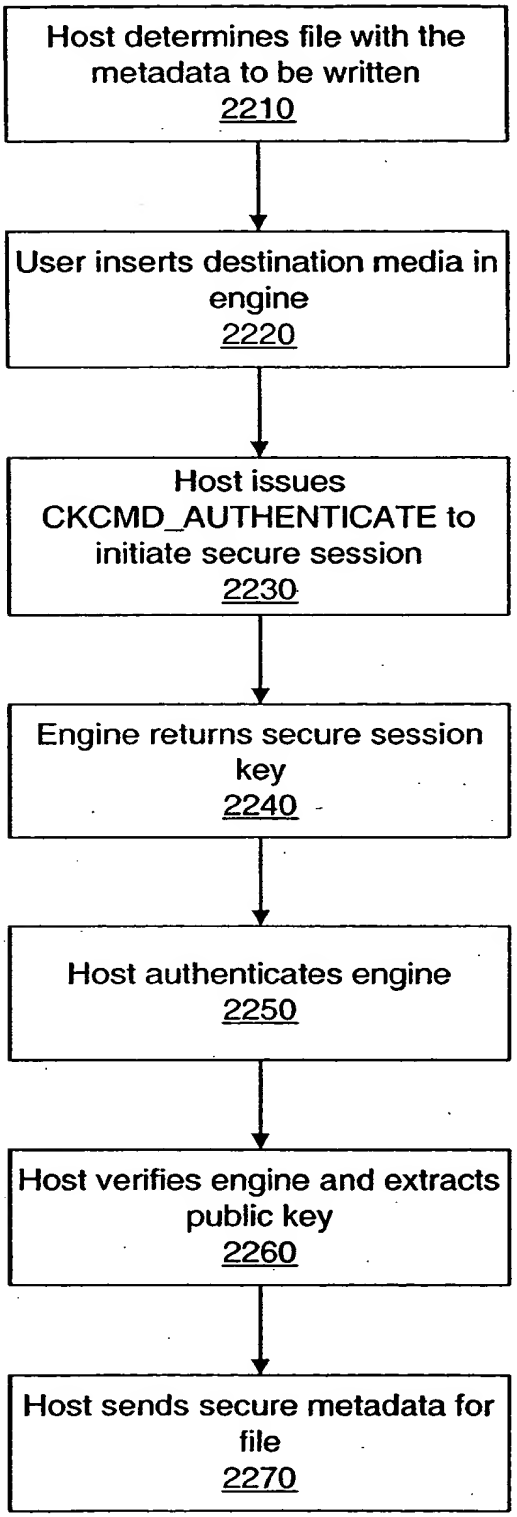

FIG. 22A

TO/2380 : 8800+50

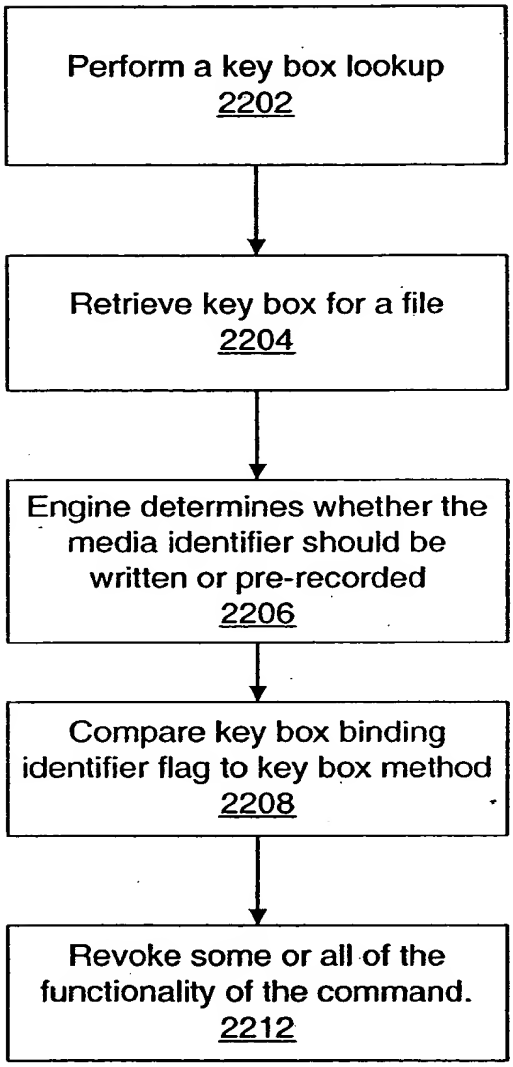

FIG. 22B

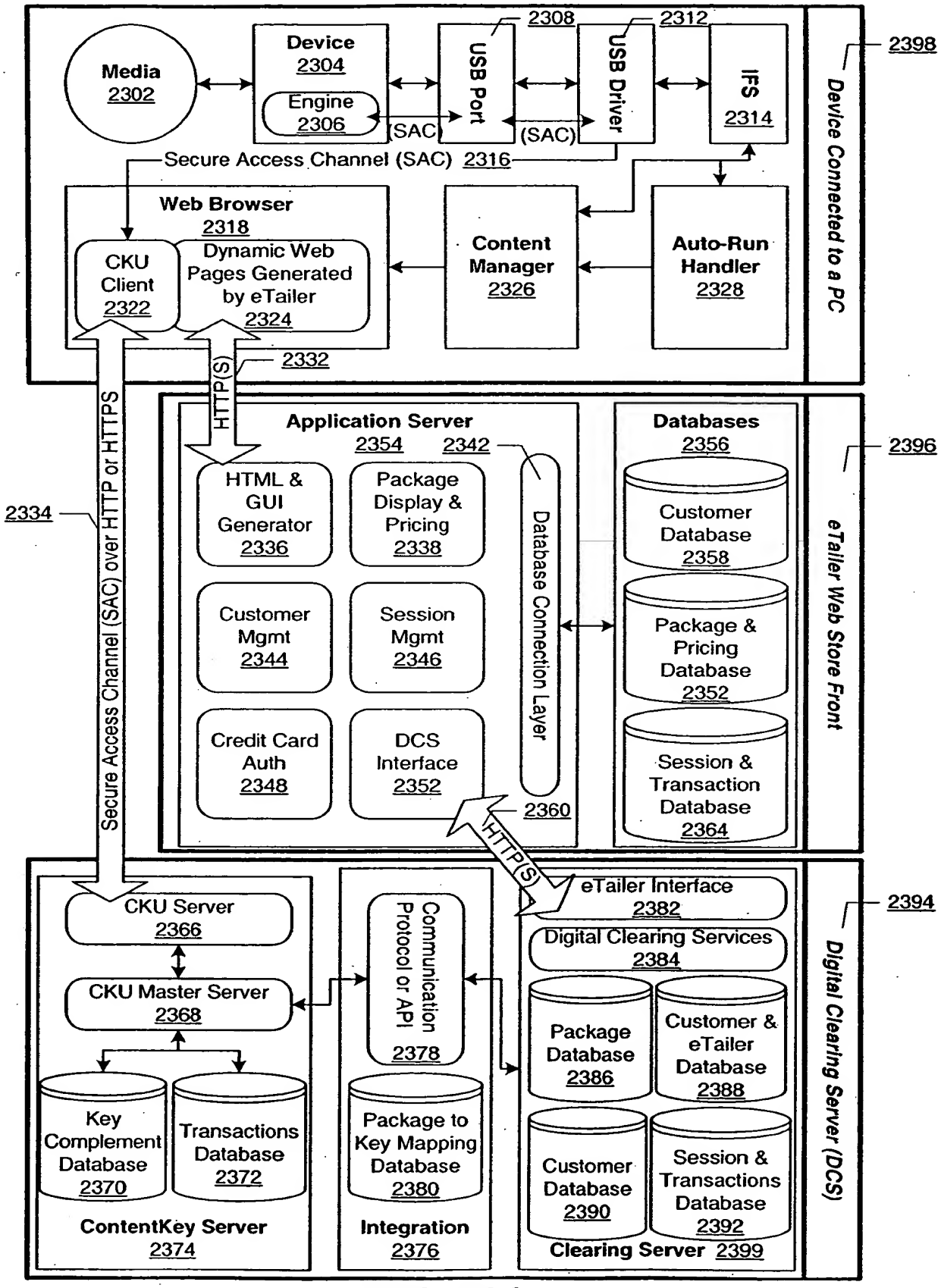

FIG. 23A

10/2004-8004660

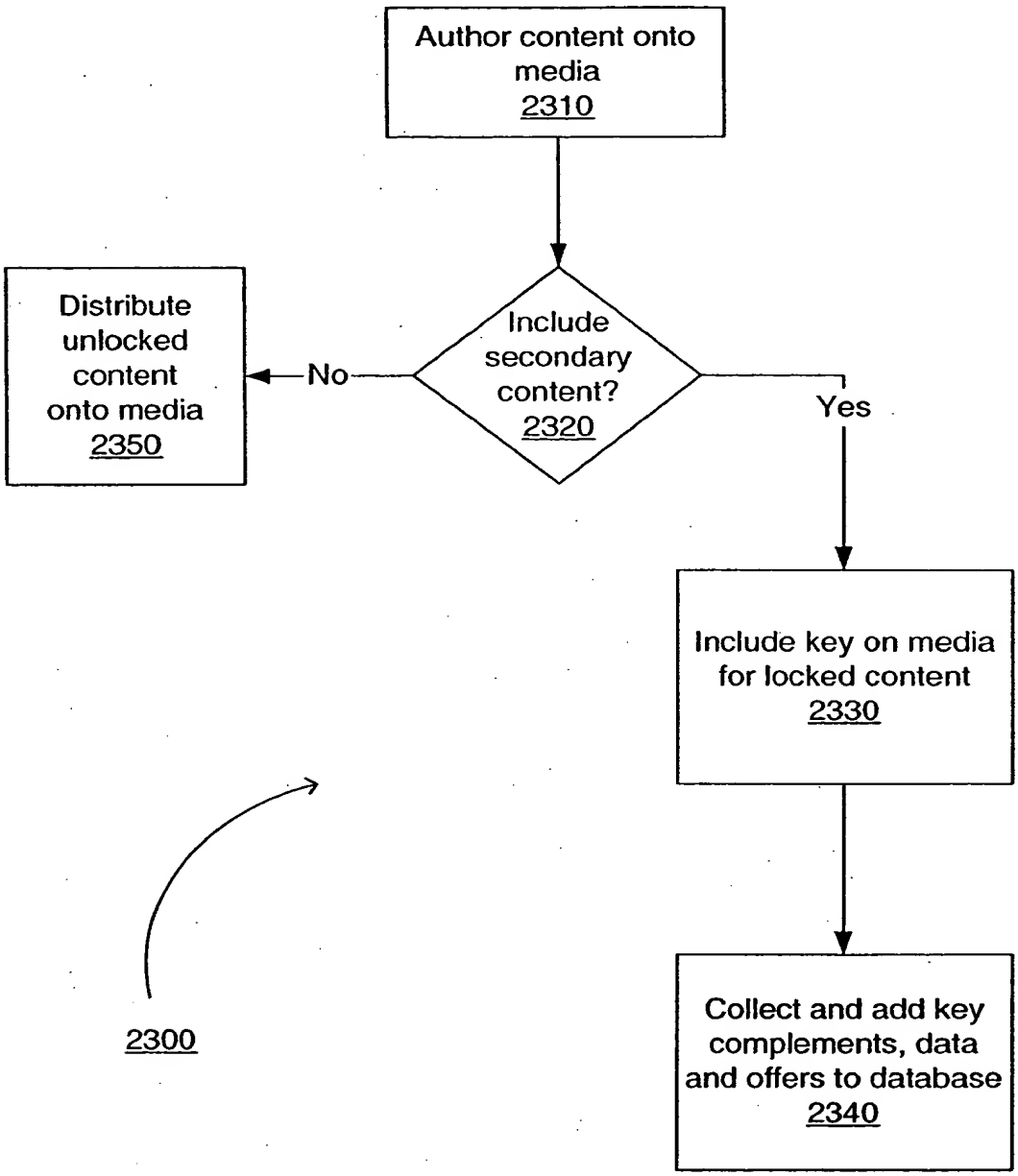
Author content onto media
2310
Include secondary content?
2320
No
Distribute unlocked content onto media
2350
Yes
Include key on media for locked content
2330
Collect and add key complements, data and offers to database
2340
2300

FIG. 23B

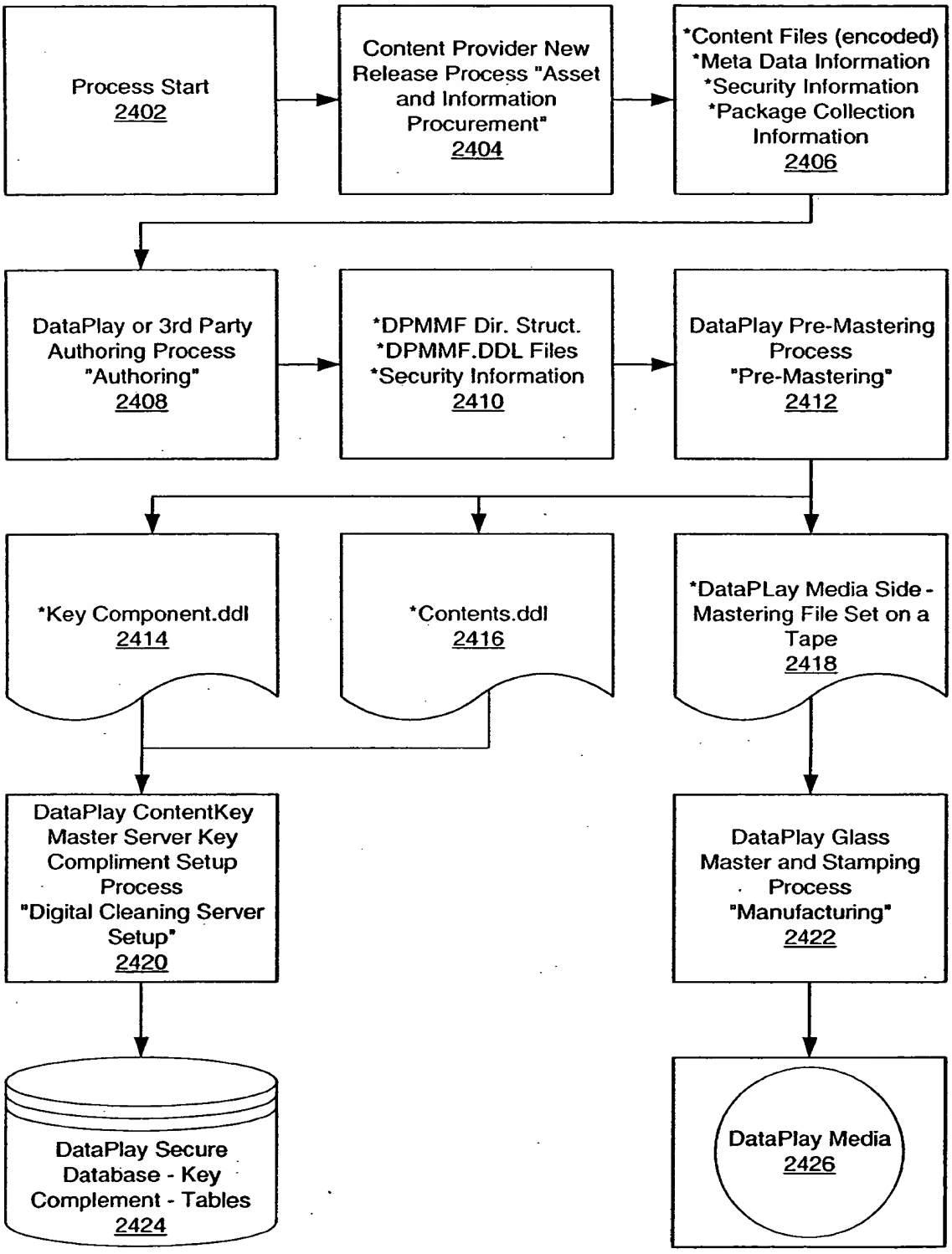

FIG. 24

Express Mail No. EV 339 908 405 US

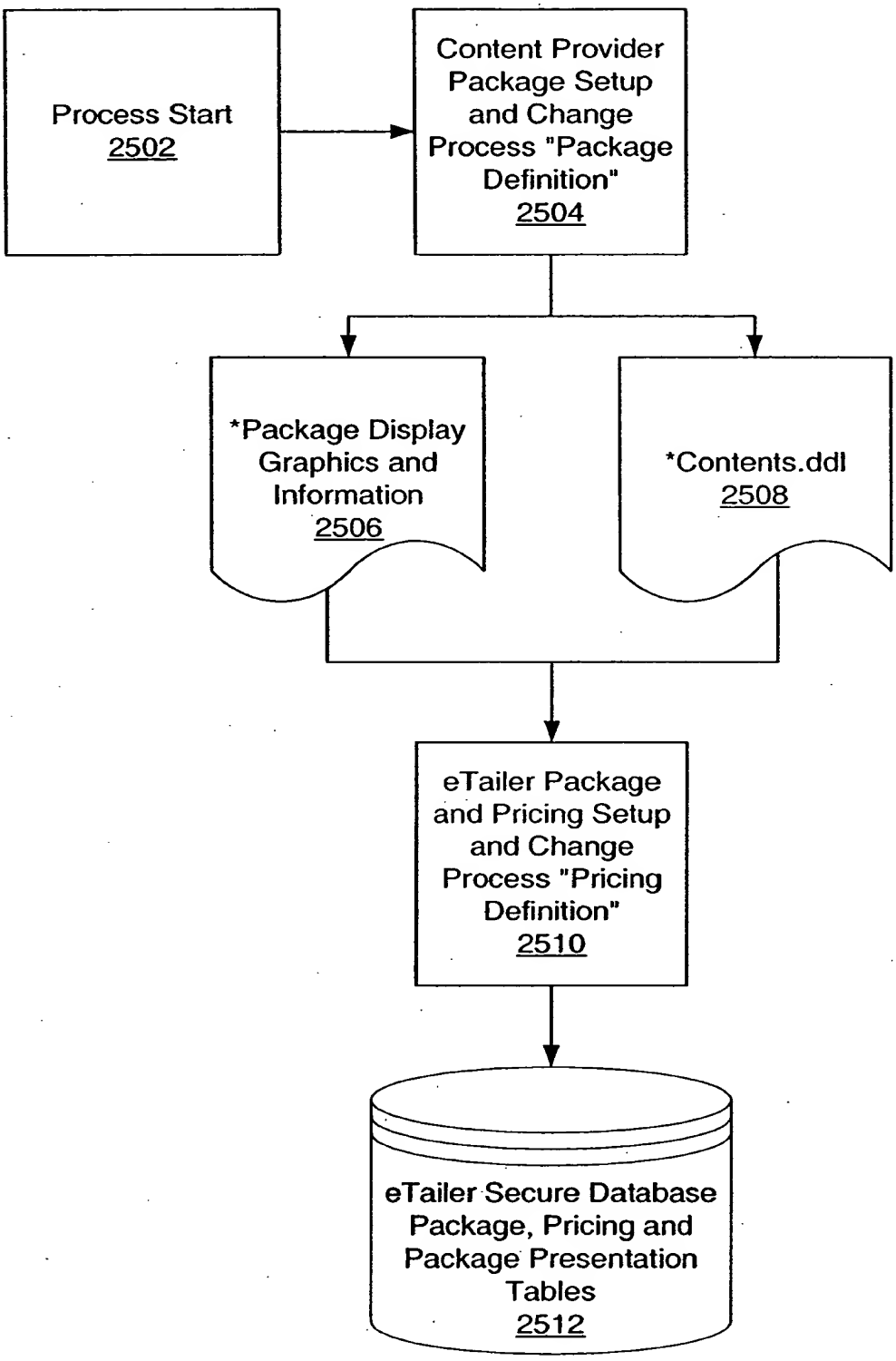

FIG. 25

TO2580: 3804660

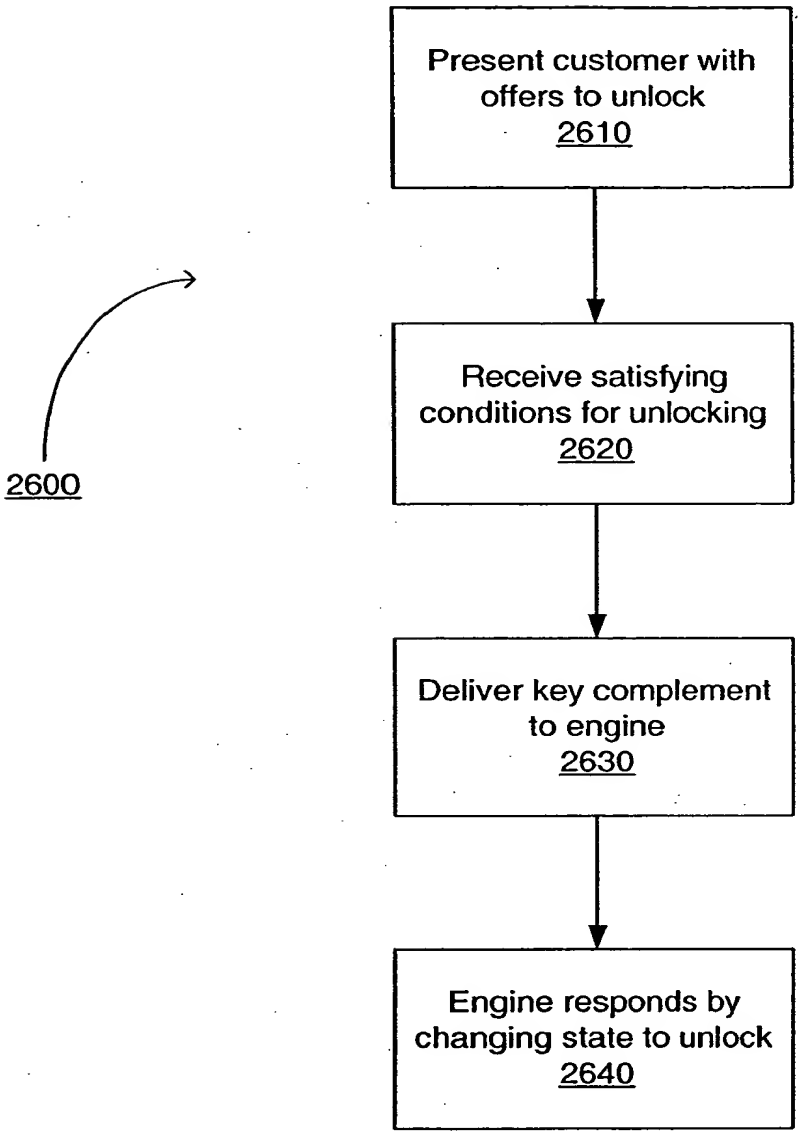

FIG. 26

Patent Application Publication Sep. 25, 2003 Sheet 26 of 95 US 2003/0182584 A1

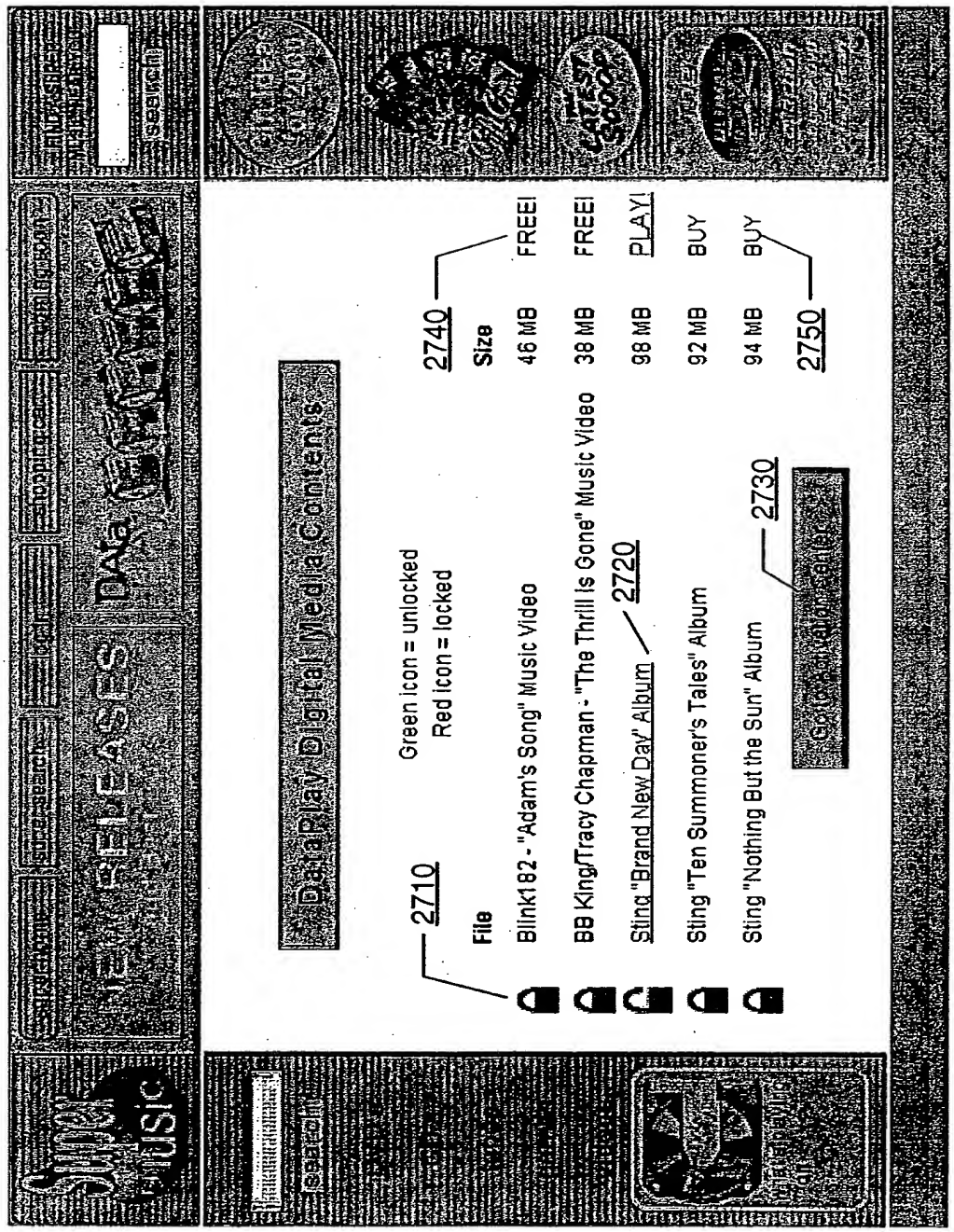
Data Play Digital Media Contents
Green icon = unlocked
Red icon = locked
File
Size
Blink182 - "Adam's Song" Music Video 46 MB FREE!
BB King/Tracy Chapman - "The Thrill Is Gone" Music Video 38 MB FREE!
Sting "Brand New Day" Album 98 MB PLAY!
Sting "Ten Summoner's Tales" Album 92 MB BUY
Sting "Nothing But the Sun" Album 94 MB BUY
2710
2720
2730
2740
2750
2700

FIG. 27

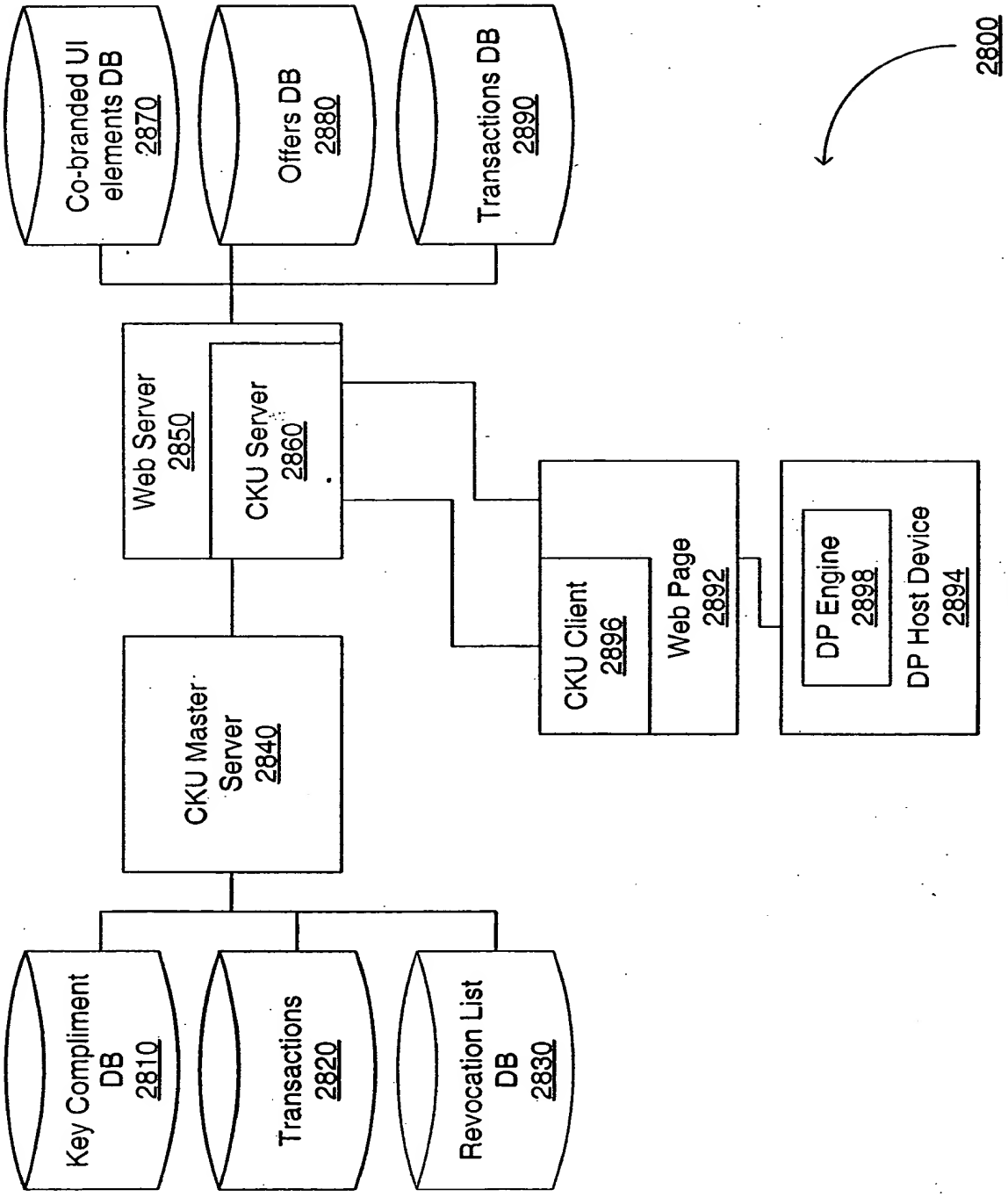
2800
Co-branded UI elements DB 2870
Offers DB 2880
Transactions DB 2890
Web Server 2850
CKU Server 2860
CKU Client 2896
Web Page 2892
DP Engine 2898
DP Host Device 2894
CKU Master Server 2840
Key Compliment DB 2810
Transactions 2820
Revocation List DB 2830

FIG. 28

T07280" E800h660

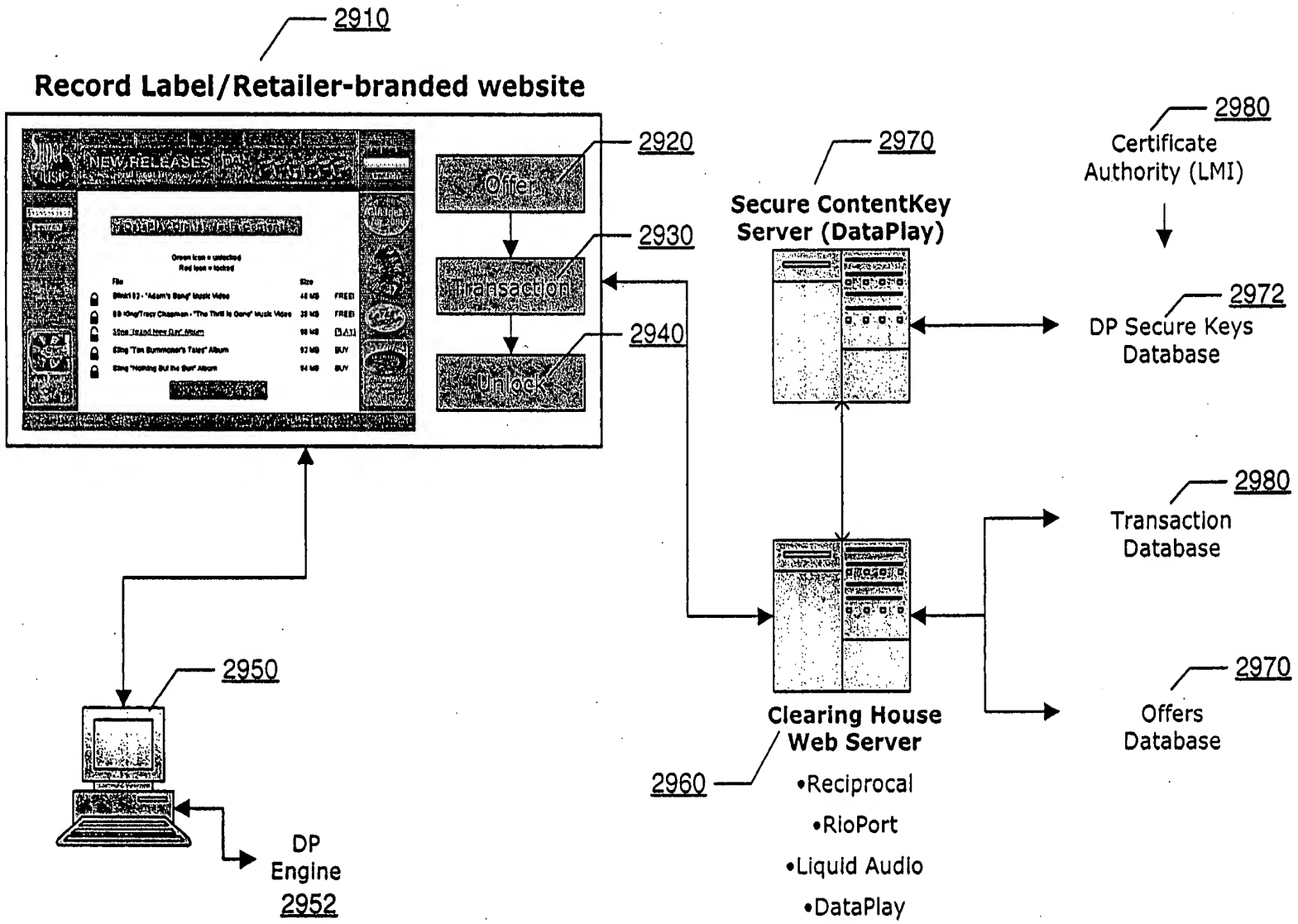

FIG. 29

Attorney Docket No.: M-9793 US
First Inventor: Timothy R. Feldman
Title: A Secure Access Method and System

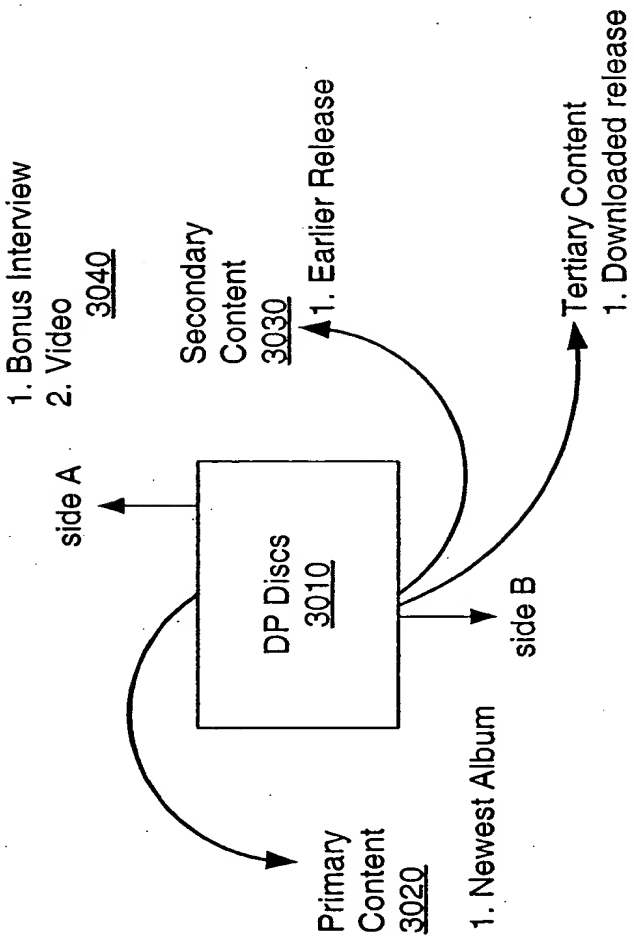
1. Bonus Interview
2. Video
3040
side A
DP Discs
3010
Secondary
Content
3030
1. Earlier Release
Tertiary Content
1. Downloaded release
side B
Primary
Content
3020
1. Newest Album

FIG. 30

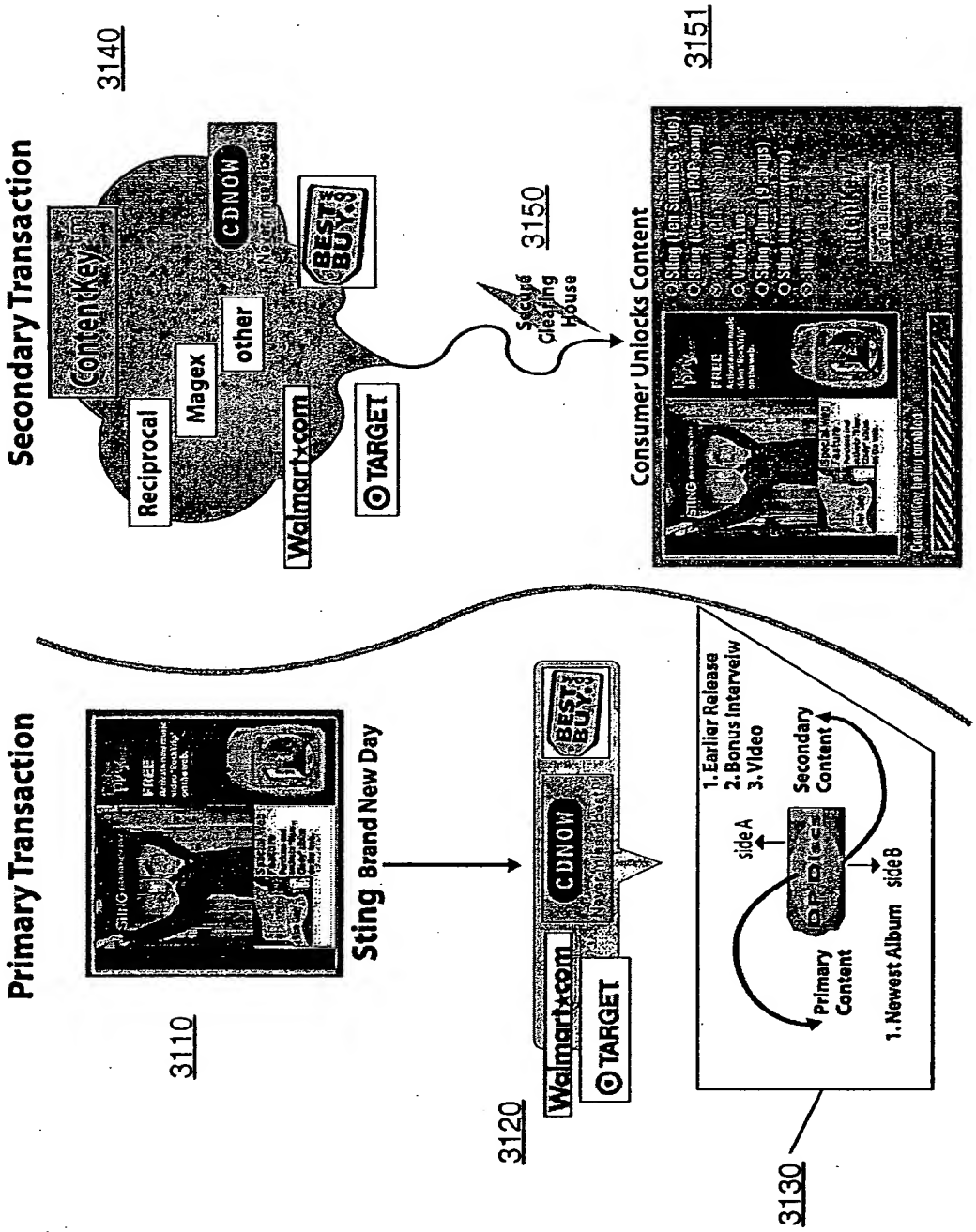
Primary Transaction
Sting Brand New Day
3110
3120
3130
Secondary Transaction
3140
ContentKey
Reciprocal
Magex
other
CDNOW
BEST BUY
Walmart.com
TARGET
Secure Clearing House
3150
Consumer Unlocks Content
3151
1. Earlier Release
2. Bonus Interview
3. Video
Secondary Content
side A
side B
Primary Content
1. Newest Album

FIG. 31A

10/736,803 09/04/2003

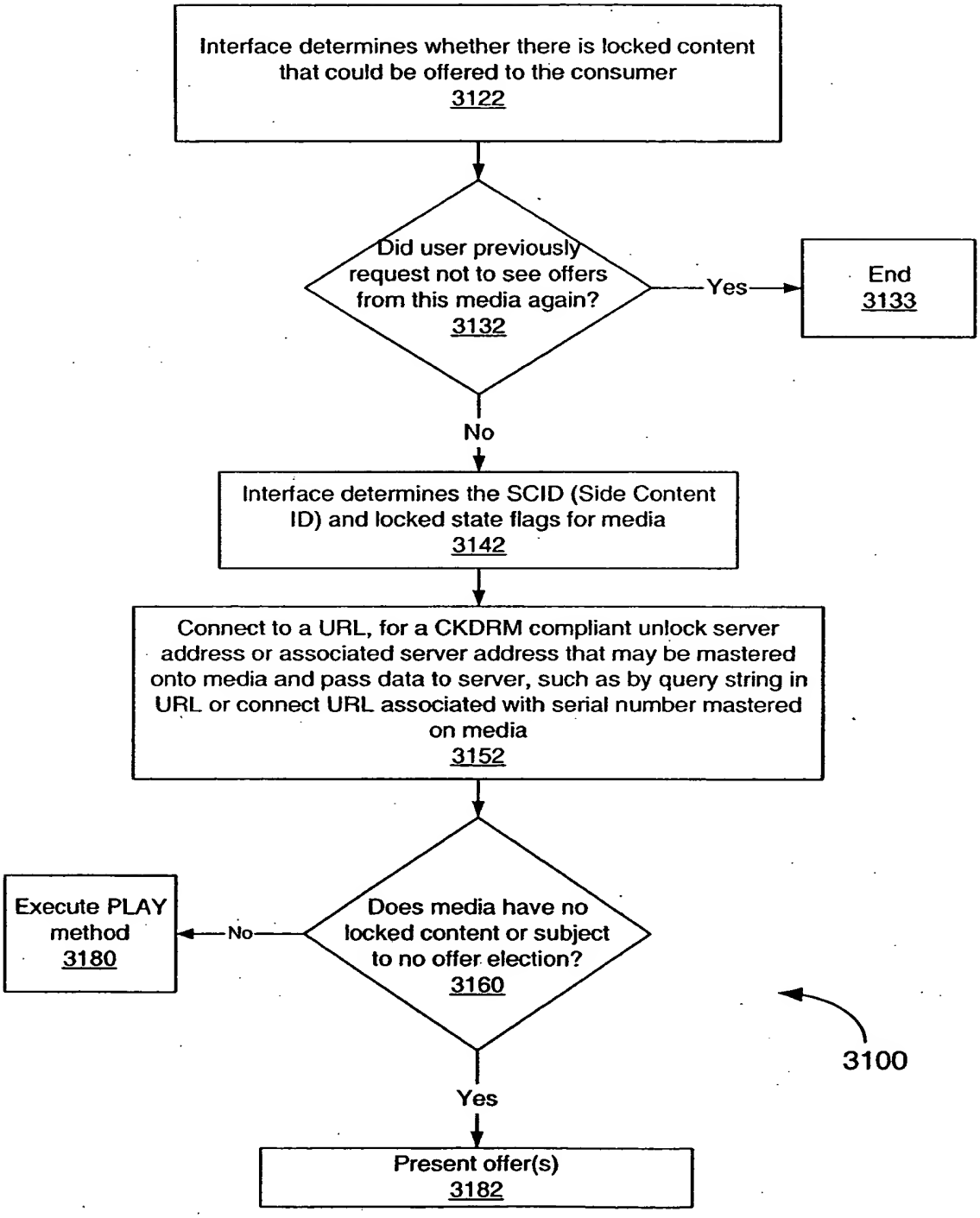

FIG. 31B

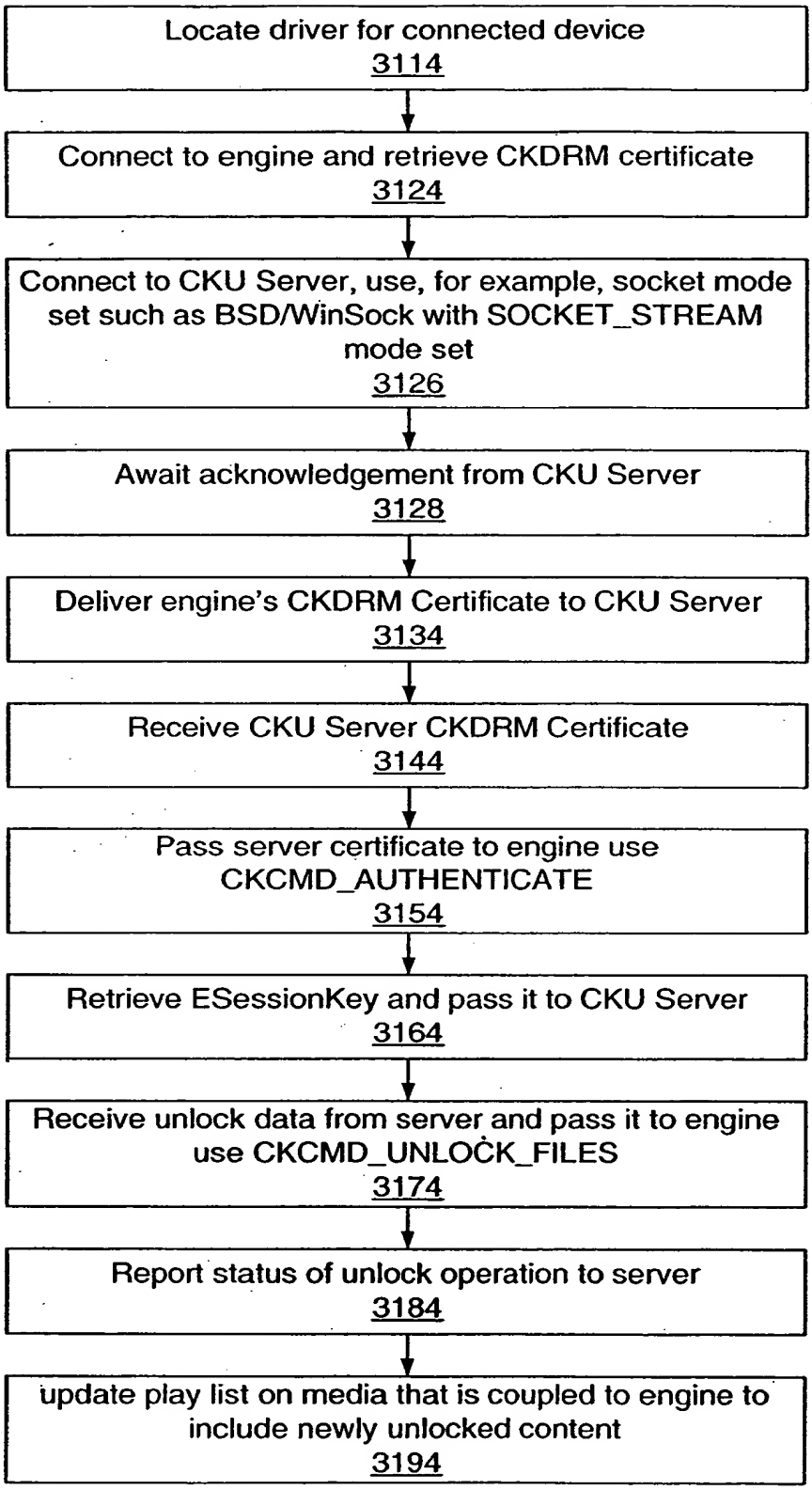

FIG. 31C

EXPRESS MAIL NO. EV 339 038 459

T07280"E800h660

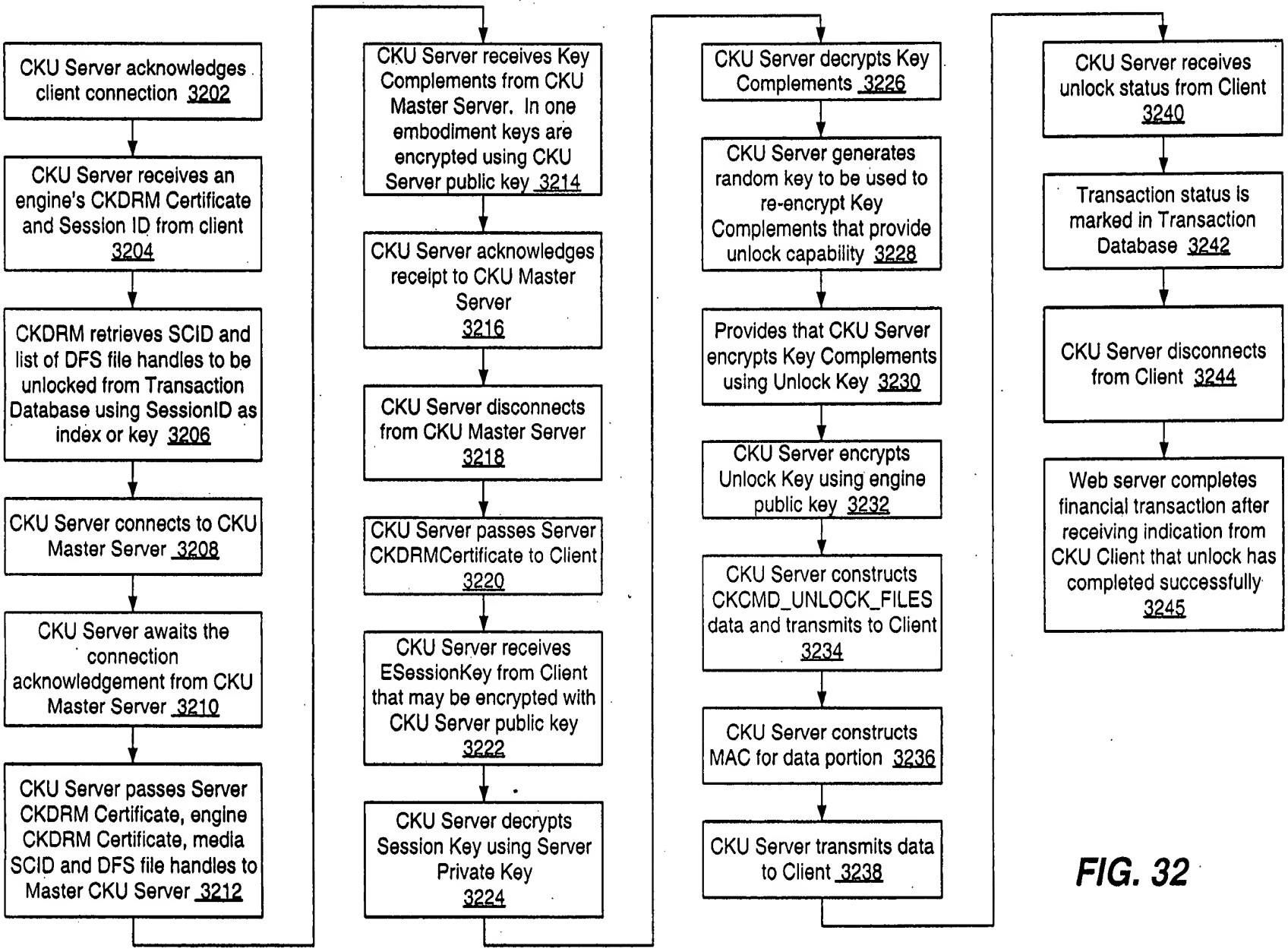

FIG. 32

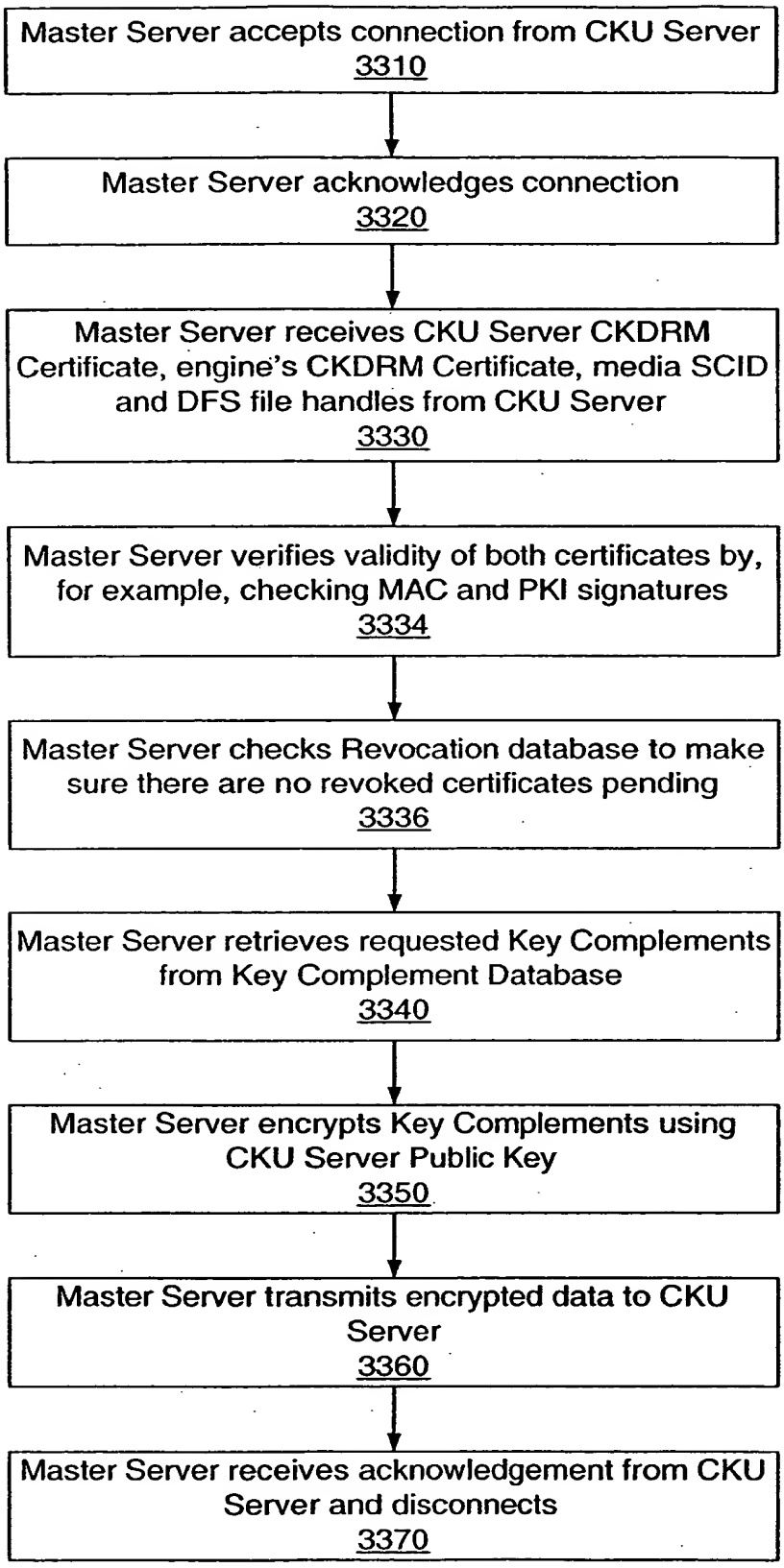

FIG. 33

EXHIBIT 1009 - Page 0094

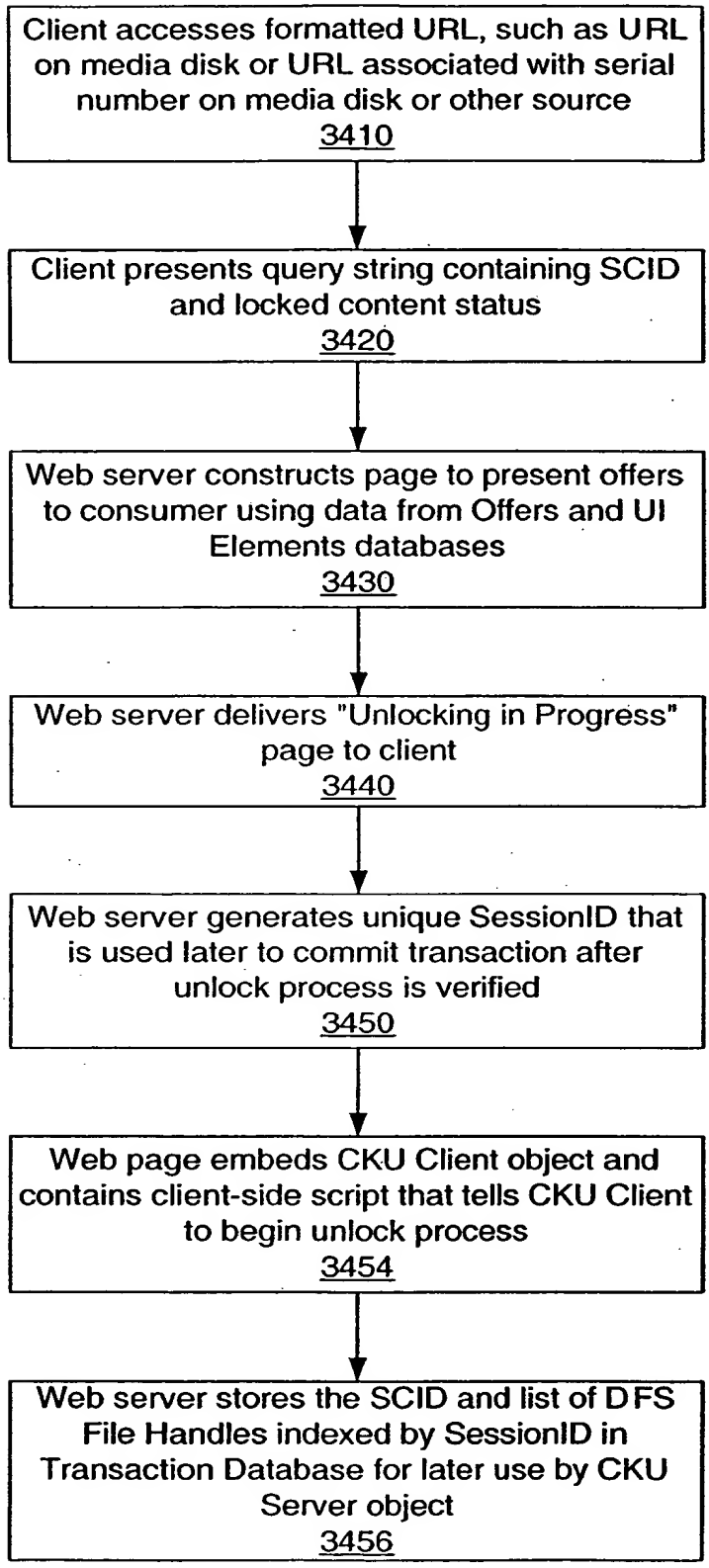

FIG. 34

EV 338045607

T07280" E800h660

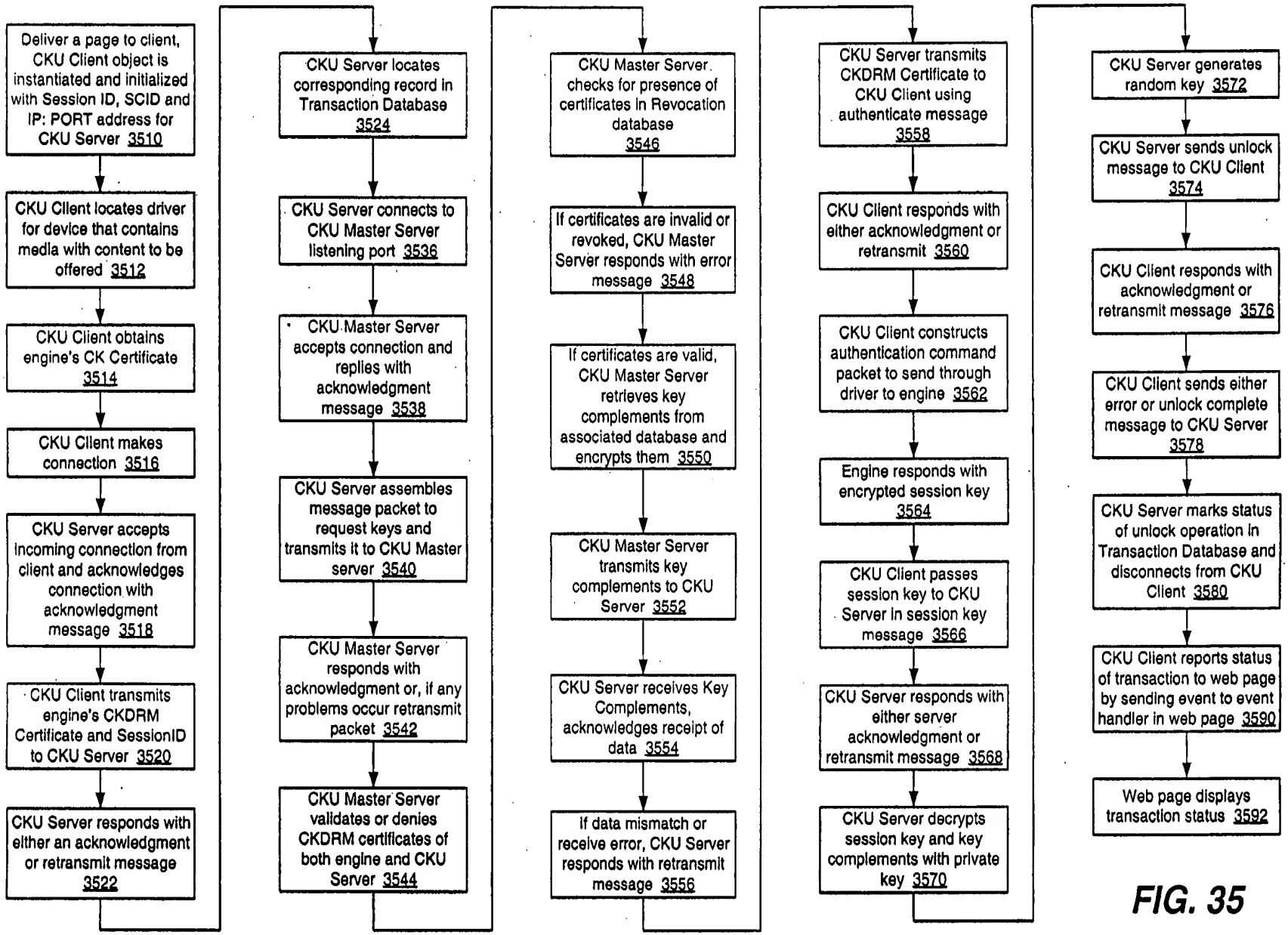

FIG. 35

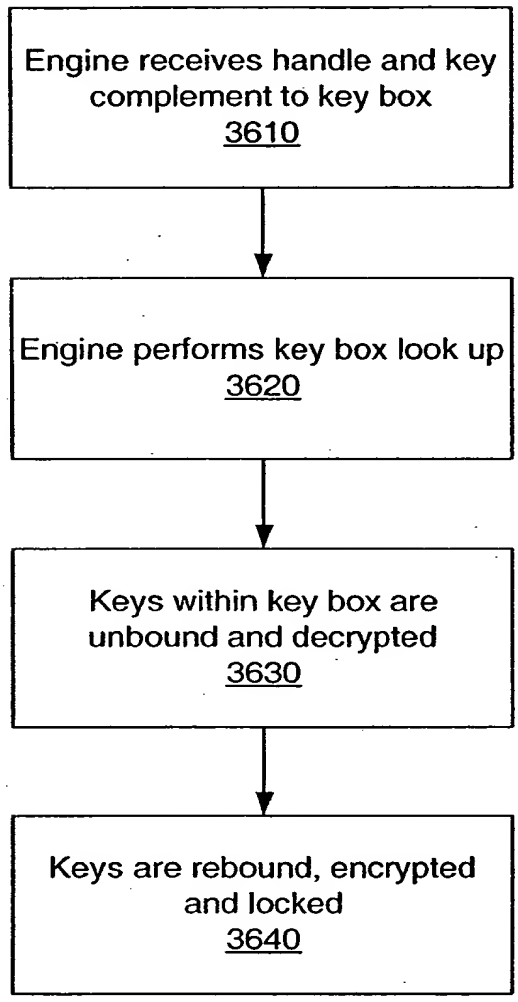

FIG. 36

TO/2680 - 3800+5.0

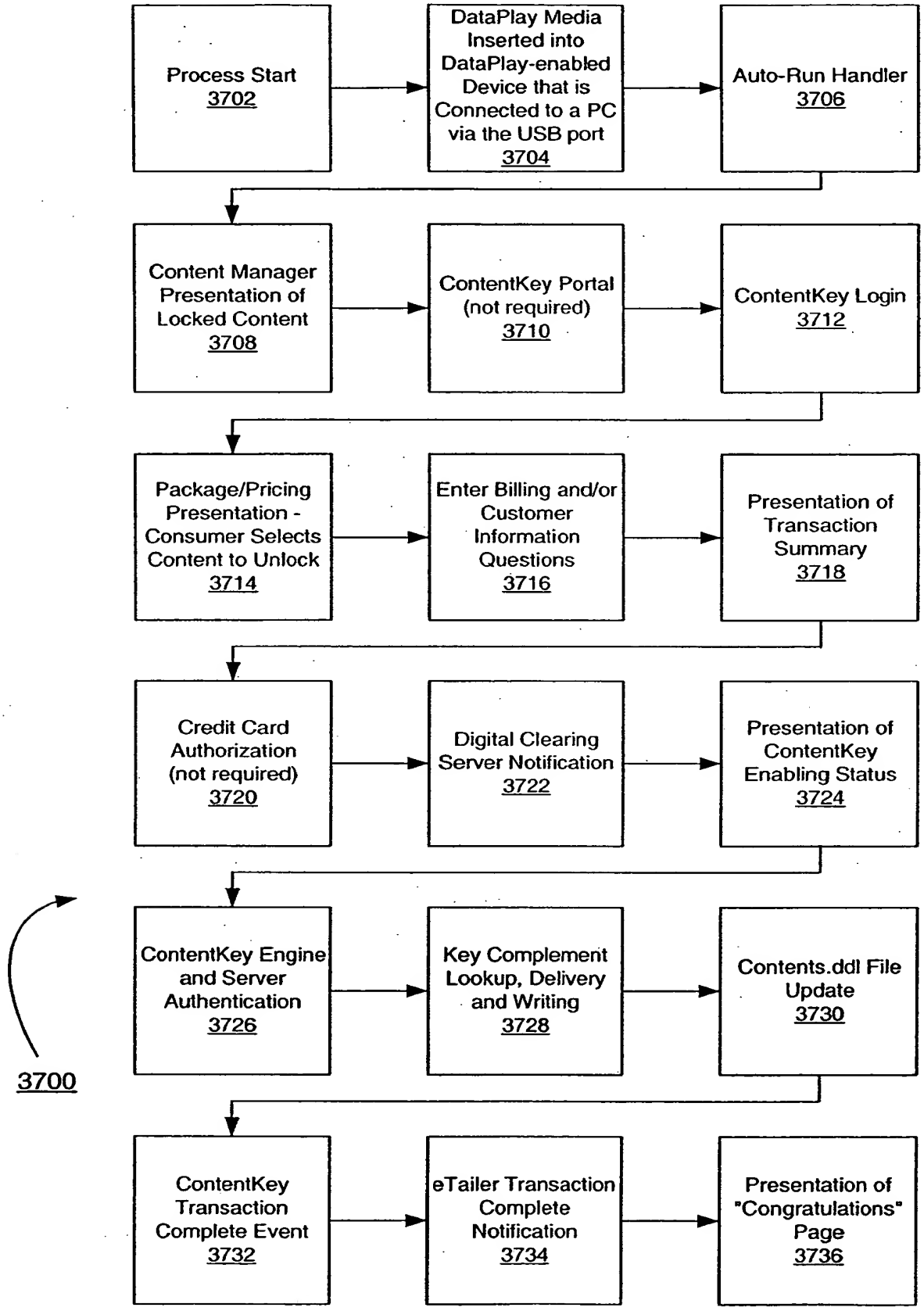

FIG. 37

10/29/2003, 3800+650

EVS980045650

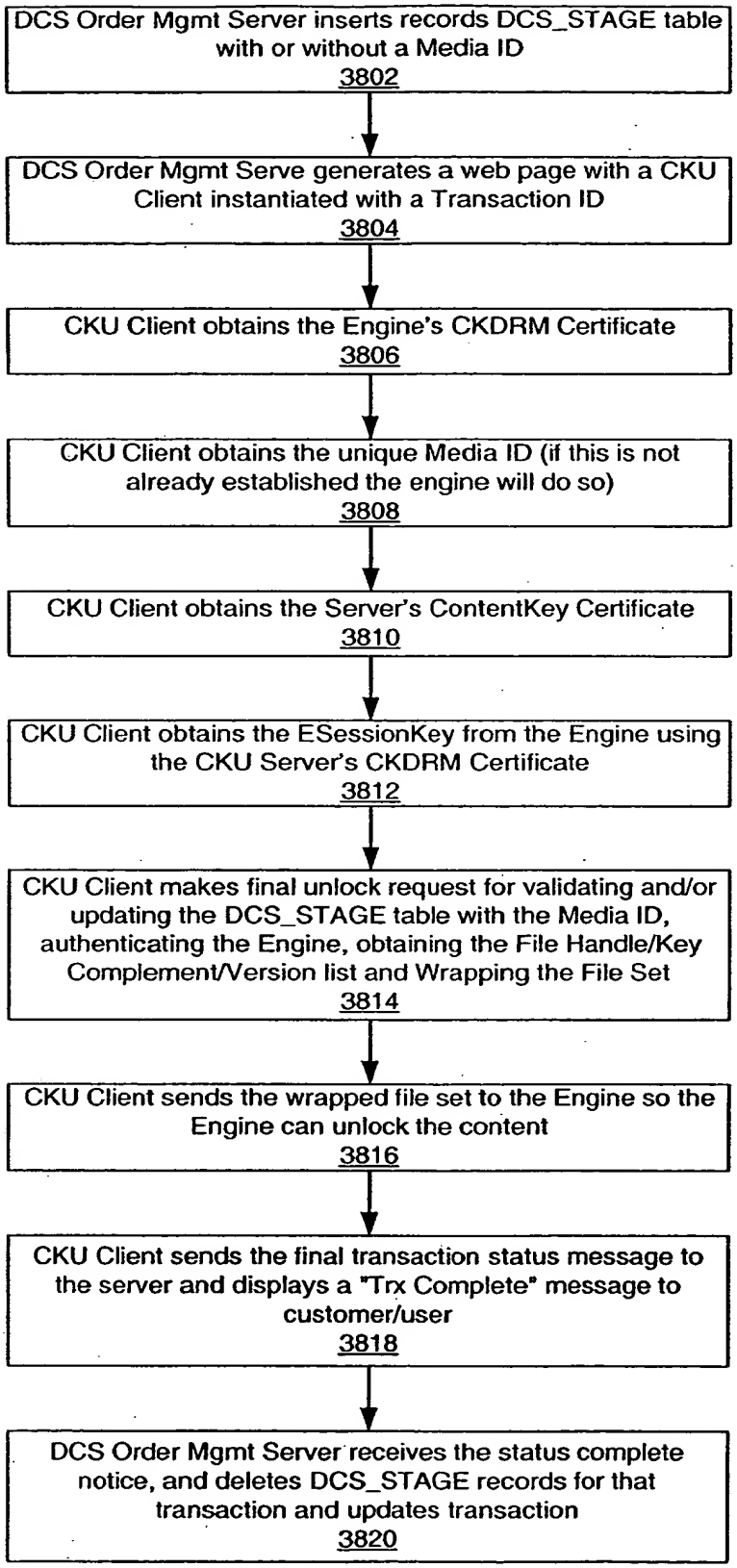

FIG. 38

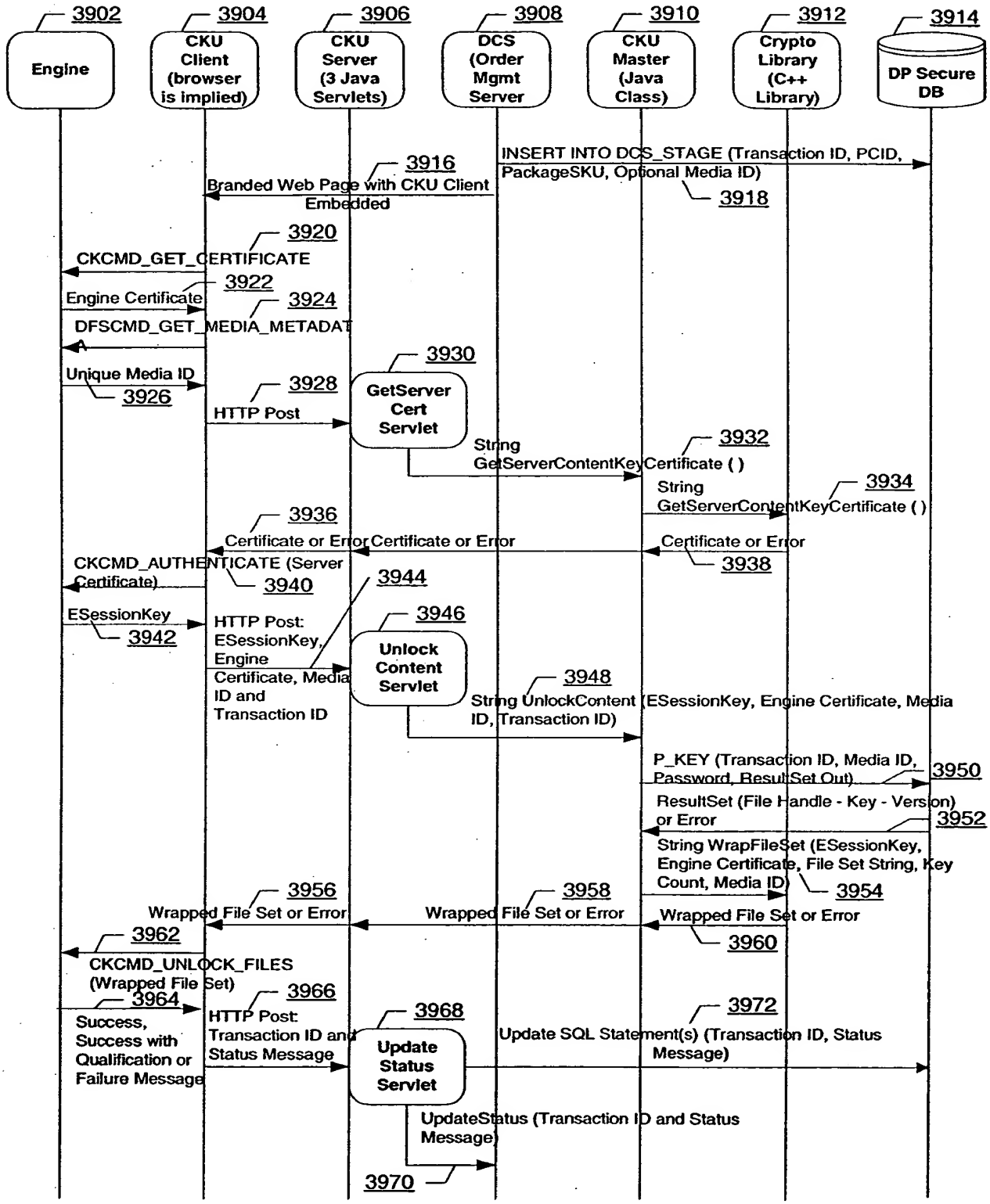
3902
Engine
3904
CKU Client (browser is implied)
3906
CKU Server (3 Java Servlets)
3908
DCS (Order Mgmt Server
3910
CKU Master (Java Class)
3912
Crypto Library (C++ Library)
3914
DP Secure DB
INSERT INTO DCS_STAGE (Transaction ID, PCID, PackageSKU, Optional Media ID)
3918
3916
Branded Web Page with CKU Client Embedded
3920
CKCMD_GET_CERTIFICATE
3922
Engine Certificate
3924
DFSCMD_GET_MEDIA_METADAT
3930
Unique Media ID
3926
3928
HTTP Post
GetServer Cert Servlet
String GetServerContentKeyCertificate ( )
3932
String GetServerContentKeyCertificate ( )
3934
3936
Certificate or Error
Certificate or Error
Certificate or Error
3938
CKCMD_AUTHENTICATE (Server Certificate)
3940
3944
ESessionKey
3942
HTTP Post: ESessionKey, Engine Certificate, Media ID and Transaction ID
3946
Unlock Content Servlet
3948
String UnlockContent (ESessionKey, Engine Certificate, Media ID, Transaction ID)
P_KEY (Transaction ID, Media ID, Password, ResultSet Out)
3950
ResultSet (File Handle - Key - Version) or Error
3952
String WrapFileSet (ESessionKey, Engine Certificate, File Set String, Key Count, Media ID)
3954
3956
Wrapped File Set or Error
3958
Wrapped File Set or Error
Wrapped File Set or Error
3960
3962
CKCMD_UNLOCK_FILES (Wrapped File Set)
3964
3966
Success, Success with Qualification or Failure Message
HTTP Post: Transaction ID and Status Message
3968
Update Status Servlet
3972
Update SQL Statement(s) (Transaction ID, Status Message)
UpdateStatus (Transaction ID and Status Message)
3970

FIG. 39

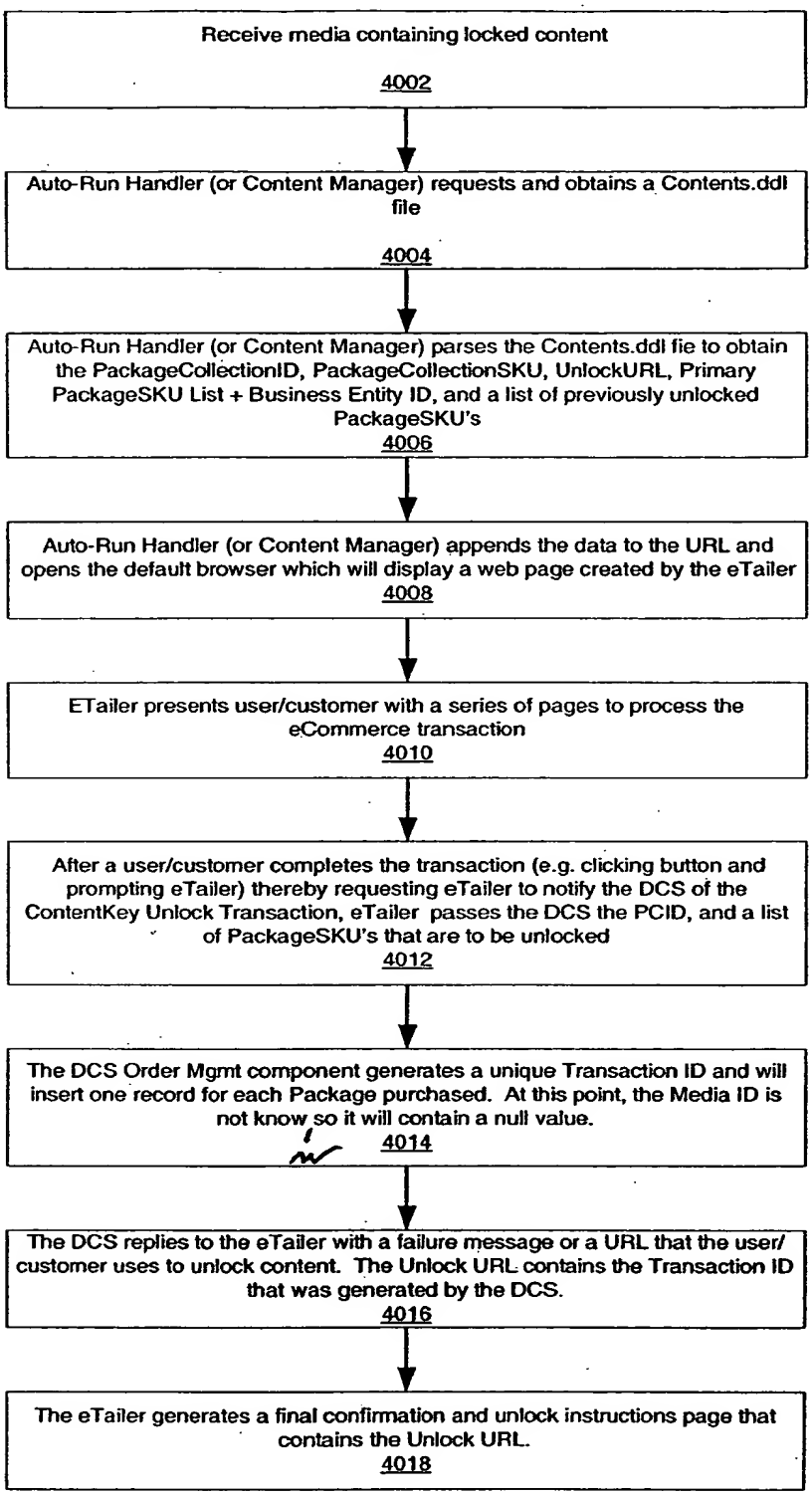

FIG. 40

EXHIBIT 1008 - Page 1050

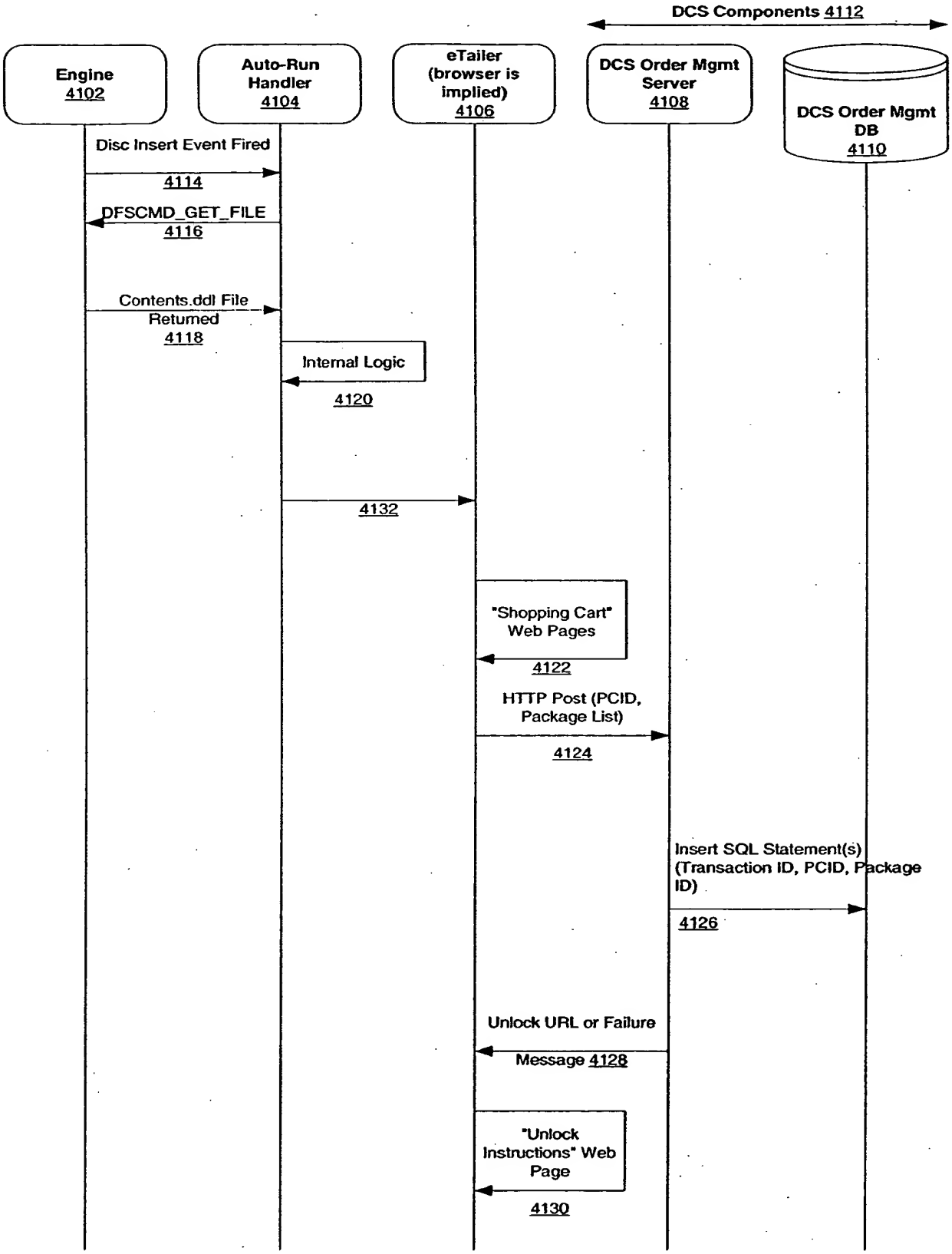

FIG. 41

10/28/2004, EAST Version: 1.4.1